SUPREME COURT OF INDIA

CIVIL WRIT PETITION 829 / 2013

IN THE MATTER OF:

S.G. VOMBATKERE & ANR. ...PETITIONERS

Versus

UNION OF INDIA & ORS. ...RESPONDENTS

COMPILATION

VOLUME IV – B

FOREIGN CASE - LAWS

(Pages 259 - 554)

(See Inside for Complete Index)

Submitted on behalf of the Petitioners

VOLUME IV

FOREIGN CASE LAWS

259

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

UNITED STATES *v.* JONES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 10–1259. Argued November 8, 2011—Decided January 23, 2012

The Government obtained a search warrant permitting it to install a Global-Positioning-System (GPS) tracking device on a vehicle registered to respondent Jones's wife. The warrant authorized installation in the District of Columbia and within 10 days, but agents installed the device on the 11th day and in Maryland. The Government then tracked the vehicle's movements for 28 days. It subsequently secured an indictment of Jones and others on drug trafficking conspiracy charges. The District Court suppressed the GPS data obtained while the vehicle was parked at Jones's residence, but held the remaining data admissible because Jones had no reasonable expectation of privacy when the vehicle was on public streets. Jones was convicted. The D. C. Circuit reversed, concluding that admission of the evidence obtained by warrantless use of the GPS device violated the Fourth Amendment.

Held: The Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment. Pp. 3–12.

(a) The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Here, the Government's physical intrusion on an "effect" for the purpose of obtaining information constitutes a "search." This type of encroachment on an area enumerated in the Amendment would have been considered a search within the meaning of the Amendment at the time it was adopted. Pp. 3–4.

(b) This conclusion is consistent with this Court's Fourth Amendment jurisprudence, which until the latter half of the 20th century was tied to common-law trespass. Later cases, which have deviated from that exclusively property-based approach, have applied the

260

Syllabus

analysis of Justice Harlan's concurrence in *Katz* v. *United States*, 389 U. S. 347, which said that the Fourth Amendment protects a person's "reasonable expectation of privacy," *id.*, at 360. Here, the Court need not address the Government's contention that Jones had no "reasonable expectation of privacy," because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, the Court must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo* v. *United States*, 533 U. S. 27, 34. *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. The *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test. See *Alderman* v. *United States*, 394 U. S. 165, 176; *Soldal* v. *Cook County*, 506 U. S. 56, 64. *United States* v. *Knotts*, 460 U. S. 276, and *United States* v. *Karo*, 468 U. S. 705—post-*Katz* cases rejecting Fourth Amendment challenges to "beepers," electronic tracking devices representing another form of electronic monitoring—do not foreclose the conclusion that a search occurred here. *New York* v. *Class*, 475 U. S. 106, and *Oliver* v. *United States*, 466 U. S. 170, also do not support the Government's position. Pp. 4–12.

(c) The Government's alternative argument—that if the attachment and use of the device was a search, it was a reasonable one—is forfeited because it was not raised below. P. 12.

615 F. 3d 544, affirmed.

SCALIA, J., delivered the opinion of the Court, in which ROBERTS, C. J., and KENNEDY, THOMAS, and SOTOMAYOR, JJ., joined. SOTOMAYOR, J., filed a concurring opinion. ALITO, J., filed an opinion concurring in the judgment, in which GINSBURG, BREYER, and KAGAN, JJ., joined.

261

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER *v.* ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE SCALIA delivered the opinion of the Court.

We decide whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment.

I

In 2004 respondent Antoine Jones, owner and operator of a nightclub in the District of Columbia, came under suspicion of trafficking in narcotics and was made the target of an investigation by a joint FBI and Metropolitan Police Department task force. Officers employed various investigative techniques, including visual surveillance of the nightclub, installation of a camera focused on the front door of the club, and a pen register and wiretap covering Jones's cellular phone.

Based in part on information gathered from these sources, in 2005 the Government applied to the United States District Court for the District of Columbia for a warrant authorizing the use of an electronic tracking device on the Jeep Grand Cherokee registered to Jones's

wife. A warrant issued, authorizing installation of the device in the District of Columbia and within 10 days.

On the 11th day, and not in the District of Columbia but in Maryland,[1] agents installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot. Over the next 28 days, the Government used the device to track the vehicle's movements, and once had to replace the device's battery when the vehicle was parked in a different public lot in Maryland. By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period.

The Government ultimately obtained a multiple-count indictment charging Jones and several alleged co-conspirators with, as relevant here, conspiracy to distribute and possess with intent to distribute five kilograms or more of cocaine and 50 grams or more of cocaine base, in violation of 21 U. S. C. §§841 and 846. Before trial, Jones filed a motion to suppress evidence obtained through the GPS device. The District Court granted the motion only in part, suppressing the data obtained while the vehicle was parked in the garage adjoining Jones's residence. 451 F. Supp. 2d 71, 88 (2006). It held the remaining data admissible, because "'[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.'" *Ibid.* (quoting *United States* v. *Knotts*, 460 U. S. 276, 281 (1983)). Jones's trial in October 2006 produced a hung jury on the conspiracy count.

In March 2007, a grand jury returned another indict-

---

[1] In this litigation, the Government has conceded noncompliance with the warrant and has argued only that a warrant was not required. *United States* v. *Maynard*, 615 F. 3d 544, 566, n. (CADC 2010).

263

ment, charging Jones and others with the same conspiracy. The Government introduced at trial the same GPS-derived locational data admitted in the first trial, which connected Jones to the alleged conspirators' stash house that contained $850,000 in cash, 97 kilograms of cocaine, and 1 kilogram of cocaine base. The jury returned a guilty verdict, and the District Court sentenced Jones to life imprisonment.

The United States Court of Appeals for the District of Columbia Circuit reversed the conviction because of admission of the evidence obtained by warrantless use of the GPS device which, it said, violated the Fourth Amendment. *United States* v. *Maynard*, 615 F. 3d 544 (2010). The D. C. Circuit denied the Government's petition for rehearing en banc, with four judges dissenting. 625 F. 3d 766 (2010). We granted certiorari, 564 U. S. ___ (2011).

II

A

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." It is beyond dispute that a vehicle is an "effect" as that term is used in the Amendment. *United States* v. *Chadwick*, 433 U. S. 1, 12 (1977). We hold that the Government's installation of a GPS device on a target's vehicle,[2] and its use of that device to monitor the vehicle's movements, constitutes a "search."

---

[2]As we have noted, the Jeep was registered to Jones's wife. The Government acknowledged, however, that Jones was "the exclusive driver." *Id.*, at 555, n. (internal quotation marks omitted). If Jones was not the owner he had at least the property rights of a bailee. The Court of Appeals concluded that the vehicle's registration did not affect his ability to make a Fourth Amendment objection, *ibid.*, and the Government has not challenged that determination here. We therefore do not consider the Fourth Amendment significance of Jones's status.

It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted. *Entick* v. *Carrington*, 95 Eng. Rep. 807 (C. P. 1765), is a "case we have described as a 'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the Constitution was adopted, and considered to be 'the true and ultimate expression of constitutional law'" with regard to search and seizure. *Brower* v. *County of Inyo*, 489 U. S. 593, 596 (1989) (quoting *Boyd* v. *United States*, 116 U. S. 616, 626 (1886)). In that case, Lord Camden expressed in plain terms the significance of property rights in search-and-seizure analysis:

> "[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law." *Entick*, *supra*, at 817.

The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to "the right of the people to be secure against unreasonable searches and seizures"; the phrase "in their persons, houses, papers, and effects" would have been superfluous.

Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century. *Kyllo* v. *United States*, 533 U. S. 27, 31 (2001); Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 816 (2004). Thus, in *Olmstead* v. *United States*, 277 U. S.

438 (1928), we held that wiretaps attached to telephone wires on the public streets did not constitute a Fourth Amendment search because "[t]here was no entry of the houses or offices of the defendants," *id.*, at 464.

Our later cases, of course, have deviated from that exclusively property-based approach. In *Katz* v. *United States*, 389 U. S. 347, 351 (1967), we said that "the Fourth Amendment protects people, not places," and found a violation in attachment of an eavesdropping device to a public telephone booth. Our later cases have applied the analysis of Justice Harlan's concurrence in that case, which said that a violation occurs when government officers violate a person's "reasonable expectation of privacy," *id.*, at 360. See, *e.g.*, *Bond* v. *United States*, 529 U. S. 334 (2000); *California* v. *Ciraolo*, 476 U. S. 207 (1986); *Smith* v. *Maryland*, 442 U. S. 735 (1979).

The Government contends that the Harlan standard shows that no search occurred here, since Jones had no "reasonable expectation of privacy" in the area of the Jeep accessed by Government agents (its underbody) and in the locations of the Jeep on the public roads, which were visible to all. But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, *supra*, at 34. As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates.[3] *Katz* did not repudiate

[3]JUSTICE ALITO's concurrence (hereinafter concurrence) doubts the wisdom of our approach because "it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case." *Post*, at 3 (opinion concurring in judgment). But in fact it posits a situation that is not far afield—a constable's concealing himself

that understanding. Less than two years later the Court upheld defendants' contention that the Government could not introduce against them conversations between *other* people obtained by warrantless placement of electronic surveillance devices in their homes. The opinion rejected the dissent's contention that there was no Fourth Amendment violation "unless the conversational privacy of the homeowner himself is invaded."[4] *Alderman* v. *United States*, 394 U. S. 165, 176 (1969). "[W]e [do not] believe that *Katz*, by holding that the Fourth Amendment protects persons and their private conversations, was intended to withdraw any of the protection which the Amendment extends to the home . . . ." *Id.*, at 180.

More recently, in *Soldal* v. *Cook County*, 506 U. S. 56 (1992), the Court unanimously rejected the argument that although a "seizure" had occurred "in a 'technical' sense" when a trailer home was forcibly removed, *id.*, at 62, no Fourth Amendment violation occurred because law enforcement had not "invade[d] the [individuals'] privacy," *id.*, at 60. *Katz*, the Court explained, established that "property rights are not the sole measure of Fourth

---

in the target's coach in order to track its movements. *Ibid.* There is no doubt that the information gained by that trespassory activity would be the product of an unlawful search—whether that information consisted of the conversations occurring in the coach, or of the destinations to which the coach traveled.

In any case, it is quite irrelevant whether there was an 18th-century analog. Whatever new methods of investigation may be devised, our task, *at a minimum*, is to decide whether the action in question would have constituted a "search" within the original meaning of the Fourth Amendment. Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.

[4]Thus, the concurrence's attempt to recast *Alderman* as meaning that individuals have a "legitimate expectation of privacy in all conversations that [take] place under their roof," *post*, at 6–7, is foreclosed by the Court's opinion. The Court took as a given that the homeowner's "conversational privacy" had not been violated.

Amendment violations," but did not "snuf[f] out the previously recognized protection for property." 506 U. S., at 64. As Justice Brennan explained in his concurrence in *Knotts*, *Katz* did not erode the principle "that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment." 460 U. S., at 286 (opinion concurring in judgment). We have embodied that preservation of past rights in our very definition of "reasonable expectation of privacy" which we have said to be an expectation "that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Minnesota* v. *Carter*, 525 U. S. 83, 88 (1998) (internal quotation marks omitted). *Katz* did not narrow the Fourth Amendment's scope.[5]

The Government contends that several of our post-*Katz* cases foreclose the conclusion that what occurred here constituted a search. It relies principally on two cases in

---

[5]The concurrence notes that post-*Katz* we have explained that "'an actual trespass is neither necessary *nor sufficient* to establish a constitutional violation.'" *Post*, at 6 (quoting *United States* v. *Karo*, 468 U. S. 705, 713 (1984)). That is undoubtedly true, and undoubtedly irrelevant. *Karo* was considering whether a seizure occurred, and as the concurrence explains, a seizure of property occurs, not when there is a trespass, but "when there is some meaningful interference with an individual's possessory interests in that property." *Post*, at 2 (internal quotation marks omitted). Likewise with a search. Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information.

Related to this, and similarly irrelevant, is the concurrence's point that, if analyzed separately, neither the installation of the device nor its use would constitute a Fourth Amendment search. See *ibid.* Of course not. A trespass on "houses" or "effects," or a *Katz* invasion of privacy, is not alone a search unless it is done to obtain information; and the obtaining of information is not alone a search unless it is achieved by such a trespass or invasion of privacy.

which we rejected Fourth Amendment challenges to "beepers," electronic tracking devices that represent another form of electronic monitoring. The first case, *Knotts*, upheld against Fourth Amendment challenge the use of a "beeper" that had been placed in a container of chloroform, allowing law enforcement to monitor the location of the container. 460 U. S., at 278. We said that there had been no infringement of Knotts' reasonable expectation of privacy since the information obtained—the location of the automobile carrying the container on public roads, and the location of the off-loaded container in open fields near Knotts' cabin—had been voluntarily conveyed to the public.[6] *Id.*, at 281–282. But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test. The holding in *Knotts* addressed only the former, since the latter was not at issue. The beeper had been placed in the container before it came into Knotts' possession, with the consent of the then-owner. 460 U. S., at 278. Knotts did not challenge that installation, and we specifically declined to consider its effect on the Fourth Amendment analysis. *Id.*, at 279, n. *Knotts* would be relevant, perhaps, if the Government were making the argument that what would otherwise be an unconstitutional search is not such where it produces only public information. The Government does not make that argument, and we know of no case that would support it.

The second "beeper" case, *United States* v. *Karo*, 468 U. S. 705 (1984), does not suggest a different conclusion. There we addressed the question left open by *Knotts*, whether the installation of a beeper in a container

[6] *Knotts* noted the "limited use which the government made of the signals from this particular beeper," 460 U. S., at 284; and reserved the question whether "different constitutional principles may be applicable" to "dragnet-type law enforcement practices" of the type that GPS tracking made possible here, *ibid.*

269

amounted to a search or seizure. 468 U. S., at 713. As in *Knotts*, at the time the beeper was installed the container belonged to a third party, and it did not come into possession of the defendant until later. 468 U. S., at 708. Thus, the specific question we considered was whether the installation "*with the consent of the original owner* constitute[d] a search or seizure . . . when the container is delivered to a buyer having no knowledge of the presence of the beeper." *Id.*, at 707 (emphasis added). We held not. The Government, we said, came into physical contact with the container only before it belonged to the defendant Karo; and the transfer of the container with the unmonitored beeper inside did not convey any information and thus did not invade Karo's privacy. See *id.*, at 712. That conclusion is perfectly consistent with the one we reach here. Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location. Cf. *On Lee* v. *United States*, 343 U. S. 747, 751–752 (1952) (no search or seizure where an informant, who was wearing a concealed microphone, was invited into the defendant's business). Jones, who possessed the Jeep at the time the Government trespassorily inserted the information-gathering device, is on much different footing.

The Government also points to our exposition in *New York* v. *Class*, 475 U. S. 106 (1986), that "[t]he exterior of a car . . . is thrust into the public eye, and thus to examine it does not constitute a 'search.'" *Id.*, at 114. That statement is of marginal relevance here since, as the Government acknowledges, "the officers in this case did *more* than conduct a visual inspection of respondent's vehicle," Brief for United States 41 (emphasis added). By attaching the device to the Jeep, officers encroached on a protected area. In *Class* itself we suggested that this would make a difference, for we concluded that an officer's momentary reaching into the interior of a vehicle did constitute a

search.[7] 475 U. S., at 114–115.

Finally, the Government's position gains little support from our conclusion in *Oliver* v. *United States*, 466 U. S. 170 (1984), that officers' information-gathering intrusion on an "open field" did not constitute a Fourth Amendment search even though it was a trespass at common law, *id.*, at 183. Quite simply, an open field, unlike the curtilage of a home, see *United States* v. *Dunn*, 480 U. S. 294, 300 (1987), is not one of those protected areas enumerated in the Fourth Amendment. *Oliver*, *supra*, at 176–177. See also *Hester* v. *United States*, 265 U. S. 57, 59 (1924). The Government's physical intrusion on such an area—unlike its intrusion on the "effect" at issue here—is of no Fourth Amendment significance.[8]

B

The concurrence begins by accusing us of applying "18th-century tort law." *Post*, at 1. That is a distortion. What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide *at*

[7]The Government also points to *Cardwell* v. *Lewis*, 417 U. S. 583 (1974), in which the Court rejected the claim that the inspection of an impounded vehicle's tire tread and the collection of paint scrapings from its exterior violated the Fourth Amendment. Whether the plurality said so because no search occurred or because the search was reasonable is unclear. Compare *id.*, at 591 (opinion of Blackmun, J.) ("[W]e fail to comprehend what expectation of privacy was infringed"), with *id.*, at 592 ("Under circumstances such as these, where probable cause exists, a warrantless examination of the exterior of a car is not unreasonable . . . ").

[8]Thus, our theory is *not* that the Fourth Amendment is concerned with "*any* technical trespass that led to the gathering of evidence." *Post*, at 3 (ALITO, J., concurring in judgment) (emphasis added). The Fourth Amendment protects against trespassory searches only with regard to those items ("persons, houses, papers, and effects") that it enumerates. The trespass that occurred in *Oliver* may properly be understood as a "search," but not one "in the constitutional sense." 466 U. S., at 170, 183.

271

a minimum the degree of protection it afforded when it was adopted. The concurrence does not share that belief. It would apply *exclusively Katz*'s reasonable-expectation-of-privacy test, even when that eliminates rights that previously existed.

The concurrence faults our approach for "present[ing] particularly vexing problems" in cases that do not involve physical contact, such as those that involve the transmission of electronic signals. *Post*, at 9. We entirely fail to understand that point. For unlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.

In fact, it is the concurrence's insistence on the exclusivity of the *Katz* test that needlessly leads us into "particularly vexing problems" in the present case. This Court has to date not deviated from the understanding that mere visual observation does not constitute a search. See *Kyllo*, 533 U. S., at 31–32. We accordingly held in *Knotts* that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." 460 U. S., at 281. Thus, even assuming that the concurrence is correct to say that "[t]raditional surveillance" of Jones for a 4-week period "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," *post*, at 12, our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.

And answering it affirmatively leads us needlessly into additional thorny problems. The concurrence posits that "relatively short-term monitoring of a person's movements

on public streets" is okay, but that "the use of longer term GPS monitoring in investigations *of most offenses*" is no good. *Post*, at 13 (emphasis added). That introduces yet another novelty into our jurisprudence. There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. See *post*, at 13–14. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist? We may have to grapple with these "vexing problems" in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.

III

The Government argues in the alternative that even if the attachment and use of the device was a search, it was reasonable—and thus lawful—under the Fourth Amendment because "officers had reasonable suspicion, and indeed probable cause, to believe that [Jones] was a leader in a large-scale cocaine distribution conspiracy." Brief for United States 50–51. We have no occasion to consider this argument. The Government did not raise it below, and the D. C. Circuit therefore did not address it. See 625 F. 3d, at 767 (Ginsburg, Tatel, and Griffith, JJ., concurring in denial of rehearing en banc). We consider the argument forfeited. See *Sprietsma* v. *Mercury Marine*, 537 U. S. 51, 56, n. 4 (2002).

* * *

The judgment of the Court of Appeals for the D. C. Circuit is affirmed.

It is so ordered.

272

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER *v.* ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE SOTOMAYOR, concurring.

I join the Court's opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, "[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area." *Ante*, at 6, n. 3. In this case, the Government installed a Global Positioning System (GPS) tracking device on respondent Antoine Jones' Jeep without a valid warrant and without Jones' consent, then used that device to monitor the Jeep's movements over the course of four weeks. The Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection. See, *e.g.*, *Silverman* v. *United States*, 365 U. S. 505, 511–512 (1961).

Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property. See, *e.g.*, *Kyllo* v. *United States*, 533 U. S. 27, 31–33 (2001). Rather, even in the absence of a trespass, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Id.*, at 33; see also *Smith* v. *Maryland*, 442 U. S. 735, 740–741 (1979); *Katz* v. *United States*, 389 U. S. 347, 361 (1967) (Harlan, J., concurring). In *Katz*, this Court enlarged its then-prevailing focus on property rights by announcing

273

that the reach of the Fourth Amendment does not "turn upon the presence or absence of a physical intrusion." *Id.*, at 353. As the majority's opinion makes clear, however, *Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it. *Ante*, at 8. Thus, "when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment." *United States* v. *Knotts*, 460 U. S. 276, 286 (1983) (Brennan, J., concurring in judgment); see also, *e.g.*, *Rakas* v. *Illinois*, 439 U. S. 128, 144, n. 12 (1978). JUSTICE ALITO's approach, which discounts altogether the constitutional relevance of the Government's physical intrusion on Jones' Jeep, erodes that longstanding protection for privacy expectations inherent in items of property that people possess or control. See *post*, at 5–7 (opinion concurring in judgment). By contrast, the trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.

Nonetheless, as JUSTICE ALITO notes, physical intrusion is now unnecessary to many forms of surveillance. *Post*, at 9–12. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. See *United States* v. *Pineda-Moreno*, 617 F. 3d 1120, 1125 (CA9 2010) (Kozinski, C. J., dissenting from denial of rehearing en banc). In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But "[s]ituations involving merely the transmission of electronic signals without trespass

274

would *remain* subject to *Katz* analysis." *Ante*, at 11. As JUSTICE ALITO incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. *Post*, at 10–11. Under that rubric, I agree with JUSTICE ALITO that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Post*, at 13.

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, *e.g.*, *People* v. *Weaver*, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. *Pineda-Moreno*, 617 F. 3d, at 1124 (opinion of Kozinski, C. J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois* v. *Lidster*, 540 U. S. 419, 426 (2004).

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net

275

result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States* v. *Cuevas-Perez*, 640 F. 3d 272, 285 (CA7 2011) (Flaum, J., concurring).

I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques. See *Kyllo*, 533 U. S., at 35, n. 2; *ante*, at 11 (leaving open the possibility that duplicating traditional surveillance "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy"). I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance," *United States* v. *Di Re*, 332 U. S. 581, 595 (1948).*

---

* *United States* v. *Knotts*, 460 U. S. 276 (1983), does not foreclose the conclusion that GPS monitoring, in the absence of a physical intrusion, is a Fourth Amendment search. As the majority's opinion notes, *Knotts* reserved the question whether "'different constitutional principles may be applicable'" to invasive law enforcement practices such as GPS tracking. See *ante*, at 8, n. 6 (quoting 460 U. S., at 284).

United States v. *Karo*, 468 U. S. 705 (1984), addressed the Fourth

276

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith*, 442 U. S., at 742; *United States* v. *Miller*, 425 U. S. 435, 443 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as JUSTICE ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post*, at 10, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases

---

Amendment implications of the installation of a beeper in a container with the consent of the container's original owner, who was aware that the beeper would be used for surveillance purposes. *Id.*, at 707. Owners of GPS-equipped cars and smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements. To the contrary, subscribers of one such service greeted a similar suggestion with anger. Quain, Changes to OnStar's Privacy Terms Rile Some Users, N. Y. Times (Sept. 22, 2011), online at http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users (as visited Jan. 19, 2012, and available in Clerk of Court's case file). In addition, the bugged container in *Karo* lacked the close relationship with the target that a car shares with its owner. The bugged container in *Karo* was stationary for much of the Government's surveillance. See 468 U. S., at 708–710. A car's movements, by contrast, are its owner's movements.

277

to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith*, 442 U. S., at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U. S., at 351–352 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision. I therefore join the majority's opinion.

278

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER *v.* ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE ALITO, with whom JUSTICE GINSBURG, JUSTICE BREYER, and JUSTICE KAGAN join, concurring in the judgment.

This case requires us to apply the Fourth Amendment's prohibition of unreasonable searches and seizures to a 21st-century surveillance technique, the use of a Global Positioning System (GPS) device to monitor a vehicle's movements for an extended period of time. Ironically, the Court has chosen to decide this case based on 18th-century tort law. By attaching a small GPS device[1] to the underside of the vehicle that respondent drove, the law enforcement officers in this case engaged in conduct that might have provided grounds in 1791 for a suit for trespass to chattels.[2] And for this reason, the Court concludes, the installation and use of the GPS device constituted a search. *Ante*, at 3–4.

---

[1] Although the record does not reveal the size or weight of the device used in this case, there is now a device in use that weighs two ounces and is the size of a credit card. Tr. of Oral Arg. 27.

[2] At common law, a suit for trespass to chattels could be maintained if there was a violation of "the dignitary interest in the inviolability of chattels," but today there must be "some actual damage to the chattel before the action can be maintained." W. Keeton, D. Dobbs, R. Keeton, & D. Owen, Prosser & Keeton on Law of Torts 87 (5th ed. 1984) (hereinafter Prosser & Keeton). Here, there was no actual damage to the vehicle to which the GPS device was attached.

279

This holding, in my judgment, is unwise. It strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial.

I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.

I

A

The Fourth Amendment prohibits "unreasonable searches and seizures," and the Court makes very little effort to explain how the attachment or use of the GPS device fits within these terms. The Court does not contend that there was a seizure. A seizure of property occurs when there is "some meaningful interference with an individual's possessory interests in that property," *United States* v. *Jacobsen*, 466 U. S. 109, 113 (1984), and here there was none. Indeed, the success of the surveillance technique that the officers employed was dependent on the fact that the GPS did not interfere in any way with the operation of the vehicle, for if any such interference had been detected, the device might have been discovered.

The Court does claim that the installation and use of the GPS constituted a search, see *ante*, at 3–4, but this conclusion is dependent on the questionable proposition that these two procedures cannot be separated for purposes of Fourth Amendment analysis. If these two procedures are analyzed separately, it is not at all clear from the Court's opinion why either should be regarded as a search. It is clear that the attachment of the GPS device was not itself a search; if the device had not functioned or if the officers had not used it, no information would have been obtained. And the Court does not contend that the use of the device constituted a search either. On the contrary, the Court

accepts the holding in *United States* v. *Knotts*, 460 U. S. 276 (1983), that the use of a surreptitiously planted electronic device to monitor a vehicle's movements on public roads did not amount to a search. See *ante*, at 7.

The Court argues—and I agree—that "we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Ante*, at 5 (quoting *Kyllo* v. *United States*, 533 U. S. 27, 34 (2001)). But it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?[3]) The Court's theory seems to be that the concept of a search, as originally understood, comprehended any technical trespass that led to the gathering of evidence, but we know that this is incorrect. At common law, any unauthorized intrusion on private property was actionable, see Prosser & Keeton 75, but a trespass on open fields, as opposed to the "curtilage" of a home, does not fall within the scope of the Fourth Amendment because private property outside the curtilage is not part of a "hous[e]" within the meaning of the Fourth Amendment. See *Oliver* v. *United States*, 466 U. S. 170 (1984); *Hester* v. *United States*, 265 U. S. 57 (1924).

B

The Court's reasoning in this case is very similar to that in the Court's early decisions involving wiretapping and electronic eavesdropping, namely, that a technical trespass followed by the gathering of evidence constitutes a

[3] The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.

281

search. In the early electronic surveillance cases, the Court concluded that a Fourth Amendment search occurred when private conversations were monitored as a result of an "unauthorized physical penetration into the premises occupied" by the defendant. *Silverman* v. *United States*, 365 U. S. 505, 509 (1961). In *Silverman*, police officers listened to conversations in an attached home by inserting a "spike mike" through the wall that this house shared with the vacant house next door. *Id.*, at 506. This procedure was held to be a search because the mike made contact with a heating duct on the other side of the wall and thus "usurp[ed] . . . an integral part of the premises." *Id.*, at 511.

By contrast, in cases in which there was no trespass, it was held that there was no search. Thus, in *Olmstead* v. *United States*, 277 U. S. 438 (1928), the Court found that the Fourth Amendment did not apply because "[t]he taps from house lines were made in the streets near the houses." *Id.*, at 457. Similarly, the Court concluded that no search occurred in *Goldman* v. *United States*, 316 U. S. 129, 135 (1942), where a "detectaphone" was placed on the outer wall of defendant's office for the purpose of overhearing conversations held within the room.

This trespass-based rule was repeatedly criticized. In *Olmstead*, Justice Brandeis wrote that it was "immaterial where the physical connection with the telephone wires was made." 277 U. S., at 479 (dissenting opinion). Although a private conversation transmitted by wire did not fall within the literal words of the Fourth Amendment, he argued, the Amendment should be understood as prohibiting "every unjustifiable intrusion by the government upon the privacy of the individual." *Id.*, at 478. See also, *e.g.*, *Silverman*, *supra*, at 513 (Douglas, J., concurring) ("The concept of 'an unauthorized physical penetration into the premises,' on which the present decision rests seems to me beside the point. Was not the wrong . . . done when the

intimacies of the home were tapped, recorded, or revealed? The depth of the penetration of the electronic device—even the degree of its remoteness from the inside of the house—is not the measure of the injury"); *Goldman*, *supra*, at 139 (Murphy, J., dissenting) ("[T]he search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment").

Katz v. *United States*, 389 U. S. 347 (1967), finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation. *Katz* involved the use of a listening device that was attached to the outside of a public telephone booth and that allowed police officers to eavesdrop on one end of the target's phone conversation. This procedure did not physically intrude on the area occupied by the target, but the *Katz* Court "repudiate[ed]" the old doctrine, *Rakas* v. *Illinois*, 439 U. S. 128, 143 (1978), and held that "[t]he fact that the electronic device employed . . . did not happen to penetrate the wall of the booth can have no constitutional significance," 389 U. S., at 353 ("[T]he reach of th[e] [Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure"); see *Rakas*, *supra*, at 143 (describing *Katz* as holding that the "capacity to claim the protection for the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place"); *Kyllo*, *supra*, at 32 ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property"). What mattered, the Court now held, was whether the conduct at issue "violated the privacy upon which [the defendant] justifiably relied while using the telephone booth." *Katz*, *supra*,

283

at 353.

Under this approach, as the Court later put it when addressing the relevance of a technical trespass, "an actual trespass is neither necessary *nor sufficient* to establish a constitutional violation." *United States* v. *Karo*, 468 U. S. 705, 713 (1984) (emphasis added). *Ibid.* ("Compar[ing] *Katz* v. *United States*, 389 U. S. 347 (1967) (no trespass, but Fourth Amendment violation), with *Oliver* v. *United States*, 466 U. S. 170 (1984) (trespass, but no Fourth Amendment violation)"). In *Oliver*, the Court wrote:

> "The existence of a property right is but one element in determining whether expectations of privacy are legitimate. 'The premise that property interests control the right of the Government to search and seize has been discredited.' *Katz*, 389 U. S., at 353, (quoting *Warden* v. *Hayden*, 387 U. S. 294, 304 (1967); some internal quotation marks omitted)." 466 U. S., at 183.

II

The majority suggests that two post-*Katz* decisions—*Soldal* v. *Cook County*, 506 U. S. 56 (1992), and *Alderman* v. *United States*, 394 U. S. 165 (1969)—show that a technical trespass is sufficient to establish the existence of a search, but they provide little support.

In *Soldal*, the Court held that towing away a trailer home without the owner's consent constituted a seizure even if this did not invade the occupants' personal privacy. But in the present case, the Court does not find that there was a seizure, and it is clear that none occurred.

In *Alderman*, the Court held that the Fourth Amendment rights of homeowners were implicated by the use of a surreptitiously planted listening device to monitor third-party conversations that occurred within their home. See 394 U. S., at 176–180. *Alderman* is best understood to

284

mean that the homeowners had a legitimate expectation of privacy in all conversations that took place under their roof. See *Rakas*, 439 U. S., at 144, n. 12 (citing *Alderman* for the proposition that "the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment"); 439 U. S., at 153 (Powell, J., concurring) (citing *Alderman* for the proposition that "property rights reflect society's explicit recognition of a person's authority to act as he wishes in certain areas, and therefore should be considered in determining whether an individual's expectations of privacy are reasonable); *Karo*, *supra*, at 732 (Stevens, J., concurring in part and dissenting in part) (citing *Alderman* in support of the proposition that "a homeowner has a reasonable expectation of privacy in the contents of his home, including items owned by others").

In sum, the majority is hard pressed to find support in post-*Katz* cases for its trespass-based theory.

III

Disharmony with a substantial body of existing case law is only one of the problems with the Court's approach in this case.

I will briefly note four others. First, the Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation). Attaching such an object is generally regarded as so trivial that it does not provide a basis for recovery under modern tort law. See Prosser & Keeton §14, at 87 (harmless or trivial contact with personal property not actionable); D. Dobbs, Law of Torts 124 (2000) (same). But under the Court's reasoning, this conduct

285

may violate the Fourth Amendment. By contrast, if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.

Second, the Court's approach leads to incongruous results. If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints.

In the present case, the Fourth Amendment applies, the Court concludes, because the officers installed the GPS device after respondent's wife, to whom the car was registered, turned it over to respondent for his exclusive use. See *ante*, at 8. But if the GPS had been attached prior to that time, the Court's theory would lead to a different result. The Court proceeds on the assumption that respondent "had at least the property rights of a bailee," *ante*, at 3, n. 2, but a bailee may sue for a trespass to chattel only if the injury occurs during the term of the bailment. See 8A Am. Jur. 2d, Bailment §166, pp. 685–686 (2009). So if the GPS device had been installed before respondent's wife gave him the keys, respondent would have no claim for trespass—and, presumably, no Fourth Amendment claim either.

Third, under the Court's theory, the coverage of the Fourth Amendment may vary from State to State. If the events at issue here had occurred in a community property State[4] or a State that has adopted the Uniform Marital

[4] See, *e.g.*, Cal. Family Code Ann. §760 (West 2004).

Property Act,[5] respondent would likely be an owner of the vehicle, and it would not matter whether the GPS was installed before or after his wife turned over the keys. In non-community-property States, on the other hand, the registration of the vehicle in the name of respondent's wife would generally be regarded as presumptive evidence that she was the sole owner. See 60 C. J. S., Motor Vehicles §231, pp. 398–399 (2002); 8 Am. Jur. 2d, Automobiles §1208, pp. 859–860 (2007).

Fourth, the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked. For example, suppose that the officers in the present case had followed respondent by surreptitiously activating a stolen vehicle detection system that came with the car when it was purchased. Would the sending of a radio signal to activate this system constitute a trespass to chattels? Trespass to chattels has traditionally required a physical touching of the property. See Restatement (Second) of Torts §217 and Comment *e* (1963 and 1964); Dobbs, *supra*, at 123. In recent years, courts have wrestled with the application of this old tort in cases involving unwanted electronic contact with computer systems, and some have held that even the transmission of electrons that occurs when a communication is sent from one computer to another is enough. See, *e.g.*, *CompuServe, Inc.* v. *Cyber Promotions, Inc.* 962 F. Supp. 1015, 1021 (SD Ohio 1997); *Thrifty-Tel, Inc.* v. *Bezenek*, 46 Cal. App. 4th 1559, 1566, n. 6 (1996). But may such decisions be followed in applying the Court's trespass theory? Assuming that what matters under the Court's theory is the law of trespass as it existed at the time of the adoption of the Fourth

[5] See Uniform Marital Property Act §4, 9A U. L. A. 116 (1998).

287

Amendment, do these recent decisions represent a change in the law or simply the application of the old tort to new situations?

IV

A

The *Katz* expectation-of-privacy test avoids the problems and complications noted above, but it is not without its own difficulties. It involves a degree of circularity, see *Kyllo*, 533 U. S., at 34, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. See *Minnesota* v. *Carter*, 525 U. S. 83, 97 (1998) (SCALIA, J., concurring). In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[6]

On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress

[6]See, *e.g.*, NPR, The End of Privacy http://www.npr.org/series/114250076/the-end-of-privacy (all Internet materials as visited Jan. 20, 2012, and available in Clerk of Court's case file); Time Magazine, Everything About You Is Being Tracked—Get Over It, Joel Stein, Mar. 21, 2011, Vol. 177, No. 11.

289

did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U. S. C. §§2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.[7] In an ironic sense, although *Katz* overruled *Olmstead*, Chief Justice Taft's suggestion in the latter case that the regulation of wiretapping was a matter better left for Congress, see 277 U. S., at 465–466, has been borne out.

B

Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.

Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States.[8] For older phones, the accuracy of the location information depends on the density of the tower network, but new "smart phones," which

[7] See Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 850–851 (2004) (hereinafter Kerr).

[8] See CTIA Consumer Info, 50 Wireless Quick Facts, http://www.ctia.org/consumer_info/index.cfm/AID/10323.

290

are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ("crowdsourcing") the speed of all such phones on any particular road.[9] Similarly, phone-location-tracking services are offered as "social" tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.

V

In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.[10] Only an investigation of unusual importance could have justified such an

---

[9]See, *e.g.*, The bright side of sitting in traffic: Crowdsourcing road congestion data, Google Blog, http://googleblog.blogspot.com/2009/08/bright-side-of-sitting-in-traffic.html.

[10]Even with a radio transmitter like those used in *United States* v. *Knotts*, 460 U. S. 276 (1983), or *United States* v. *Karo*, 468 U. S. 705 (1984), such long-term surveillance would have been exceptionally demanding. The beepers used in those cases merely "emit[ted] periodic signals that [could] be picked up by a radio receiver." *Knotts*, 460 U.S., at 277. The signal had a limited range and could be lost if the police did not stay close enough. Indeed, in *Knotts* itself, officers lost the signal from the beeper, and only "with the assistance of a monitoring device located in a helicopter [was] the approximate location of the signal . . . picked up again about one hour later." *Id.*, at 278.

291

expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. See, *e.g.*, Kerr, 102 Mich. L. Rev., at 805–806. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.

To date, however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes. The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.

Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See *Knotts*, 460 U. S., at 281–282. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveil

lance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant.[11] We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.

* * *

For these reasons, I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment. I therefore agree with the majority that the decision of the Court of Appeals must be affirmed.

---

[11] In this case, the agents obtained a warrant, but they did not comply with two of the warrant's restrictions: They did not install the GPS device within the 10-day period required by the terms of the warrant and by Fed. Rule Crim. Proc. 41(e)(2)(B)(i), and they did not install the GPS device within the District of Columbia, as required by the terms of the warrant and by 18 U. S. C. §3117(a) and Rule 41(b)(4). In the courts below the Government did not argue, and has not argued here, that the Fourth Amendment does not impose these precise restrictions and that the violation of these restrictions does not demand the suppression of evidence obtained using the tracking device. See, *e.g.*, *United States* v. *Gerber*, 994 F. 2d 1556, 1559–1560 (CA11 1993); *United States* v. *Burke*, 517 F. 2d 377, 386–387 (CA2 1975). Because it was not raised, that question is not before us.

293

CONSEIL CONSTITUTIONNEL

Decision no. 2012-652 DC of 22 March 2012

Identity Protection Act

In the conditions provided for by Article 61-2 of the Constitution, the Constitutional Council was seized of an application relating to the Identity Protection Act on 7 March 2012 by Mr François REBSAMEN, Ms Jacqueline ALQUIER, Ms Michèle ANDRÉ, Messrs Alain ANZIANI, David ASSOULINE, Bertrand AUBAN, Dominique BAILLY, Ms Delphine BATAILLE, Messrs Claude BÉRIT-DÉBAT, Michel BERSON, Jean BESSON, Ms Maryvonne BLONDIN, Messrs Yannick BOTREL, Martial BOURQUIN, Ms Bernadette BOURZAI, Ms Nicole BRICQ, Messrs Jean-Pierre CAFFET, Pierre CAMANI, Ms Claire-Lise CAMPION, Messrs Jean-Louis CARRÈRE, Luc CARVOUNAS, Bernard CAZEAU, Yves CHASTAN, Jacques CHIRON, Ms Karine CLAIREAUX, Mr Gérard COLLOMB, Ms Hélène CONWAY MOURET, Messrs Jacques CORNANO, Roland COURTEAU, Jean-Pierre DEMERLIAT, Ms Christiane DEMONTÈS, Messrs Claude DILAIN, Claude DOMEIZEL, Ms Odette DURIEZ, Ms Frédérique ESPAGNAC, Messrs Jean-Luc FICHET, Jean-Jacques FILLEUL, Ms Catherine GÉNISSON, Samia GHALI, Messrs Jean-Pierre GODEFROY, Claude HAUT, Edmond HERVÉ, Claude JEANNEROT, Ronan KERDRAON, MS Virginie KLÈS, Messrs Jacky LE MENN, Alain LE VERN, Jean-Yves LECONTE, Ms Marie-Noëlle LIENEMANN, Messrs Jeanny LORGEOUX, Jacques-Bernard MAGNER, François MARC, Marc MASSION, Ms Michelle MEUNIER, Ms Danielle MICHEL, Messrs Jean—Pierre MICHEL, Gérard MIQUEL, Jean-Jacques MIRASSOU, Thani MOHAMED SOILIHI, Jean-Marc PASTOR, François PATRIAT, Daniel PERCHERON, Bernard PIRAS, Ms Gisèle PRINTZ, Messrs Daniel RAOUL, Thierry REPENTIN, Roland RIES, Gilbert ROGER,

Ms Patricia SCHILLINGER, Messrs Jean-Pierre SUEUR, Simon SUTOUR, Michel TESTON, René TEULADE, Richard YUNG, Ms Leila AÏCHI, Ms Esther BENBASSA, Messrs Ronan DANTEC, André GATTOLIN, Joël LABBÉ, Jean-Vincent PLACÉ, Ms Aline ARCHIMBAUD, Marie-Christine BLANDIN, Corinne BOUCHOUX, Messrs Jean DESESSARD, Jacques MÉZARD, Pierre-Yves COLLOMBAT, Robert TROPEANO, Jean-Claude REQUIER, Jean-Pierre PLANCADE, Yvon COLLIN, Ms Anne-Marie ESCOFFIER, Messrs François FORTASSIN, Raymond VALL, Jean-Michel BAYLET, Ms Françoise LABORDE, Ms Nicole BORVO COHEN-SEAT, Ms Eliane ASSASSI, Ms Marie-France BEAUFILS, Mr Eric BOCQUET, Ms Laurence COHEN, Ms Cécile CUKIERMAN, Ms Annie DAVID, Ms Michelle DEMESSINE, Ms Evelyne DIDIER, Messrs Christian FAVIER, Guy FISCHER, Thierry FOUCAUD, Ms Brigitte GONTHIER-MAURIN, Messrs Gérard LE CAM, Michel LE SCOUARNEC, Ms Isabelle PASQUET, Ms Mireille SCHURCH and Mr Paul VERGÈS, senators;

And on the same day by Mr Jean-Marc AYRAULT, Ms Patricia

ADAM, Messrs Jean-Paul BACQUET, Dominique BAERT, Jean-Pierre BALLIGAND, Gérard BAPT, Ms Delphine BATHO, Ms Marie-Noëlle BATTISTEL, Messrs Jean-Louis BIANCO, Serge BLISKO, Daniel BOISSERIE, Ms Marie-Odile BOUILLÉ, Ms Monique BOULESTIN, Messrs Pierre BOURGUIGNON, Jérôme CAHUZAC, Jean-Christophe CAMBADÉLIS, Thierry CARCENAC, Laurent CATHALA, Guy CHAMBEFORT, Jean-Paul CHANTEGUET, Gérard CHARASSE, Alain CLAEYS, Ms Marie-Françoise CLERGEAU, Messrs Pierre COHEN, Frédéric CUVILLIER, Pascal DEGUILHEM, Guy DELCOURT, Bernard DEROSIER, Julien DRAY, Tony DREYFUS, William DUMAS, Ms Laurence DUMONT, Messrs Jean-Paul DUPRÉ, Olivier DUSSOPT, Christian ECKERT, Henri EMMANUELLI, Ms Corinne ERHEL, Ms Martine FAURE, Mr Hervé FÉRON, Ms Aurélie

294

CONSEIL CONSTITUTIONNEL

FILIPPETTI, Ms Geneviève FIORASO, Messrs Pierre FORGUES, Jean-Louis GAGNAIRE, Ms Geneviève GAILLARD, Messrs Guillaume GAROT, Paul GIACOBBI, Jean-Patrick GILLE, Ms Annick GIRARDIN, Messrs Joël GIRAUD, Daniel GOLDBERG, Ms Pascale GOT, Messrs Marc GOUA, Jean GRELLIER, Ms Elisabeth GUIGOU, Mr David HABIB, Ms Danièle HOFFMAN-RISPAL, Ms Sandrine HUREL, Ms Françoise IMBERT, Messrs Michel ISSINDOU, Serge JANQUIN, Henri JIBRAYEL, Régis JUANICO, Armand JUNG, Ms Marietta KARAMANLI, Messrs Jean-Pierre KUCHEIDA, Jérôme LAMBERT, Jack LANG, Ms Colette LANGLADE, Messrs Jean-Yves LE BOUILLONNEC, Gilbert LE BRIS, Jean-Marie LE GUEN, Bruno LE ROUX, Ms Marylise LEBRANCHU, Messrs Michel LEFAIT, Patrick LEMASLE, Ms Catherine LEMORTON, Ms Annick LEPETIT, Messrs Bernard LESTERLIN, Michel LIEBGOTT, François LONCLE, Jean MALLOT, Jean-René MARSAC, Philippe MARTIN, Ms Martine MARTINEL, Ms Frédérique MASSAT, Mr Didier MATHUS, Ms Sandrine MAZETIER, Messrs Kléber MESQUIDA, Jean MICHEL, Arnaud MONTEBOURG, Pierre-Alain MUET, Philippe NAUCHE, Henri NAYROU, Christian PAUL, Germinal PEIRO, Jean-Luc PÉRAT, Jean-Claude PEREZ, Ms Sylvia PINEL, Mr François PUPPONI, Ms Catherine QUÉRÉ, Messrs Dominique RAIMBOURG, Simon RENUCCI, Ms Marie-Line REYNAUD, Ms Chantal ROBIN-RODRIGO, Messrs Marcel ROGEMONT, Bernard ROMAN, Gwendal ROUILLARD, René ROUQUET, Christophe SIRUGUE, Jean-Louis TOURAINE, Philippe TOURTELIER, Jean-Jacques URVOAS, Daniel VAILLANT, Jacques VALAX, Alain VIDALIES, Jean-Michel VILLAUMÉ and Philippe VUILQUE, Members of Parliament.

THE CONSTITUTIONAL COUNCIL,

Having regard to Ordinance no. 58-1067 of 7 November 1958 as amended, concerning the basic law on the Constitutional Council;

Having regard to Act n° 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties;

Having regard to the observations of the Government in response to the application and its complementary observations submitted upon request by the Constitutional Council, registered on 15 March 2012;

Having regard to the observations in response filed by the applicant senators, filed on 20 March 2012;

Having heard the rapporteur;

1. Considering that the applicant members of Parliament and senators have submitted the Identity Protection Act to the Constitutional Council; that they object that the provisions of Articles 5 and 10 of that act are unconstitutional;

- WITH RESPECT TO ARTICLES 5 and 10:

2. Considering that Article 5 of the act referred provides for the establishment, in the conditions provided for under the aforementioned act of 6 January 1978, of a database containing personal data in order to facilitate the collection and conservation of the data required for the issue of French passports and national identity cards which is intended to maintain the integrity of these data; that these include the data contained in the secure electronic chip on the national identity card and passport as listed in Article 2 of the act which include, in addition to the marital status and residence of the holder, its height, eye colour, fingerprints and photograph;

3. Considering that Article 5 enables an applicant for an identity or travel document to be identified by consulting the database containing personal data through the data listed in Article 2, with the exception of the photograph; that it also

CONSEIL CONSTITUTIONNEL

provides that the database containing personal data may be consulted using two fingerprints collected in the database, first upon issue of identity and travel documents, secondly for investigative requirements relating to certain offences if authorised by the public prosecutor or the examining judge, and thirdly upon request by the public prosecutor in order to establish the identity of a deceased person who has fallen victim to a natural disaster or a collective accident, if it is unknown;

4. Considering that Article 6 of the act referred enables the identity of the holder or an identity card or passport to be verified on the basis of the data reported on the identity or travel document or on the secure electronic chip; that it also enables this verification to be carried out by consulting the data conserved in the database provided for under Article 5 in the event that there is a serious doubt as to the identity of the person or where the document presented is defective or appears to have been damaged or modified;

5. Considering that Article 10 enables officers who have been individually designated and duly authorised from the national police and *gendarmerie* departments to gain access to the database containing personal data established pursuant to Article 5 for the purpose of preventing or punishing attacks against the independence of the Nation, its territorial integrity, its security, the republican form of its institutions, its defence or diplomatic service, to safeguard its population in France and abroad and the essential elements of its scientific and economic potential, and to prevent or punish acts of terrorism;

6. Considering that, according to the applicants, the establishment of a biometric database covering almost all of the French population, the characteristics of which enable a person to be identified on the basis of its fingerprints, amounts to an unconstitutional breach of the right to respect for private life; that moreover, in permitting the information contained in this database to be consulted for administrative purposes or by the investigating police, Parliament failed to adopt legal guarantees against the risk of arbitrary action;

7. Considering in the first place that Article 34 of the Constitution provides that the act shall specify the rules relating to the fundamental guarantees to be afforded to citizens for the purpose of exercising public freedoms as well as in relation to criminal procedure; that it is for Parliament, acting within the bounds of its competence, to ensure that a balance is struck on the one hand between the safeguarding of public order and bringing offenders to justice, both of which are necessary in order to uphold principles and rights of constitutional standing, and on the other hand the respect for other rights and freedoms protected under constitutional law; that it is at any time at liberty to adopt new provisions which may appear appropriate to it and to amend earlier texts or to repeal and replace them, as the case may be, with other provisions, provided that when exercising this power it does not impinge upon the legal guarantees of constitutional standing;

8. Considering, secondly, that the freedom proclaimed under Article 2 of the 1789 Declaration of the Rights of Man and the Citizen implies the right to respect for private life; that accordingly, the collection, registration, conservation, consultation and communication of personal data must be justified on grounds of general interest and implemented in an adequate manner, proportionate to this objective;

9. Considering that the establishment of a database containing personal data intended to maintain the integrity of the data necessary for the issue of identity and travel documents makes it possible to render the issue of these documents more secure and to improve the efficiency of the fight against fraud; that it is accordingly justified on grounds of general interest;

10. Considering however that, given its object, this database containing personal data is intended to collect data

CONSEIL CONSTITUTIONNEL

relating to almost all of the population of French nationality; that since the biometric data registered in this file, including in particular fingerprints, are themselves liable to be compared with physical traces left involuntarily by an individual or collected unbeknown to him, they are particularly sensitive; that the technical characteristics of this database as defined by the contested provisions enable it to be consulted for purposes other than the verification of an individual's identity; that the provisions of the act referred authorise this database to be consulted or viewed not only in relation to the issue or renewal of identity and travel documents or to verify the holder of such a document, but also for other purposes of an administrative nature or by the investigating police;

11. Considering that according to the above, having regard to the nature of the data registered, the scope of this processing, its technical characteristics and the conditions under which it may be consulted, the provisions of Article 5 violate the right to respect for privacy in a manner which cannot be regarded as proportionate to the goal pursued; that accordingly, Articles 5 and 10 of the act must be ruled unconstitutional; that the same applies, in consequence, to the third subparagraph of article 6, Article 7 and the second phrase of Article 8;

- WITH RESPECT TO ARTICLE 3:

12. Considering that Article 3 of the act referred establishes a new function for the national identity card; that pursuant to that article: If requested by its holder, the national identity card may also contain data, stored separately, enabling it to identify itself on electronic communication networks and to affix its electronic signature. Upon each use, the interested party shall decide which identification data are to be transmitted electronically.

The fact that an identity card does not have the functions described in the first subparagraph does not constitute legitimate grounds for refusal to sell or to provide services pursuant to Article L. 122-1 of the Consumer Code or to deny access to the banking operations mentioned under Article L. 311-1 of the Monetary and Financial Code.

Access to the electronic administration services implemented by the State, the local authorities or their groupings cannot be limited solely to the holders of a national identity card having the functions described in the first subparagraph of this Article;

13. Considering that, according to Article 34 of the Constitution, legislation shall determine the rules concerning: civil rights and the fundamental guarantees afforded to citizens for the exercise of their civil liberties; that it shall also determine the fundamental principles of civil and commercial obligations; that under the current state of means of communication and having regard to the general development of online communication services for the public as well as the importance of these services in economic and social life, the general conditions under which the national identity card issued by the State may enable a person to identify itself on electronic communication networks and to affix its electronic signature, in particular for civil and commercial purposes, directly pertain to the rules and principles cited above, and accordingly fall within the purview of the law;

14. Considering that Article 3 on the one hand permits the national identity card to include electronic functions enabling its holder to identify itself on electronic communication networks and to affix its electronic signature, whilst on the other hand guarantees the optional nature of these functions; that the provisions of Article 3 do not specify either the nature of the data through which these functions may be implemented or the guarantees ensuring the integrity and confidentiality of this data; that they do not define in any greater detail the conditions under which the persons implementing these functions are to be authenticated, especially when they are minors or are subject to legal protection; that accordingly, Parliament acted in excess of its powers; that accordingly Article 3 must be ruled unconstitutional;

297

CONSEIL CONSTITUTIONNEL

15. Considering that there are no grounds for the Constitutional Council to raise *ex officio* any other question concerning compatibility with the Constitution,

HELD :

Article 1 .- The following provisions of the Identity Protection Act are hereby ruled unconstitutional:

- Articles 3, 5, 7 and 10;

- the third subparagraph of Article 6;

- the second phrase of Article 8.

Article 2 .- This decision shall be published in the Journal officiel of the French Republic.

Deliberated by the Constitutional Council in its session on 22 March 2012, sat on by: Mr Jean-Louis DEBRÉ, President, Mr Jacques BARROT, Ms Claire BAZY MALAURIE, Messrs Guy CANIVET, Michel CHARASSE, Renaud DENOIX de SAINT MARC, Valéry GISCARD d'ESTAING, Ms Jacqueline de GUILLENCHMIDT, and Messrs Hubert HAENEL and Pierre STEINMETZ.

298

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KLAYMAN et al.,

Plaintiffs,

v.

OBAMA et al.,

Defendants.

Civil Action No. 13-0851 (RJL)

KLAYMAN et al.,

Plaintiff,

v.

OBAMA et al.,

Defendants.

MEMORANDUM OPINION

December 16, 2013 [Dkt. # 13 (No. 13-0851), # 10 (No. 13-0881)]

On June 6, 2013, plaintiffs brought the first of two related lawsuits challenging the constitutionality and statutory authorization of certain intelligence-gathering practices by the United States government relating to the wholesale collection of the phone record metadata of all U.S. citizens.[1] These related cases are two of several lawsuits[2] arising

[1] Plaintiffs' second suit was filed less than a week later on June 12, 2013, and challenged the constitutionality and statutory authorization of the government's collection of both phone and internet metadata records.

[2] The complaint in *ACLU v. Clapper*, Civ. No. 13-3994, which was filed in the United States District Court for the Southern District of New York on June 11, 2013, alleges claims similar to

from public revelations over the past six months that the federal government, through the National Security Agency ("NSA"), and with the participation of certain telecommunications and internet companies, has conducted surveillance and intelligence-gathering programs that collect certain data about the telephone and internet activity of American citizens within the United States. Plaintiffs—five individuals in total between No. 13-851 ("*Klayman I*") and No. 13-881 ("*Klayman II*")—bring these suits as U.S. citizens who are subscribers or users of certain telecommunications and internet firms. *See* Second Am. Compl. (*Klayman I*) [Dkt. # 37] ¶ 1; Am. Compl. (*Klayman II*) [Dkt. # 30] ¶ 1.[3] They bring suit against both federal government defendants (several federal agencies and individual executive officials) and private defendants (telecommunications and internet firms and their executive officers), alleging statutory and constitutional violations. *See generally* Second Am. Compl. (*Klayman I*); Am. Compl. (*Klayman II*).

Before the Court are plaintiffs' two Motions for Preliminary Injunction [Dkt. # 13 (*Klayman I*), # 10 (*Klayman II*)], one in each case. As relief, plaintiffs seek an injunction "that, during the pendency of this suit, (i) bars [d]efendants from collecting [p]laintiffs'

---

those in the instant two cases. *See also In re Electronic Privacy Information Center*, No. 13-58 (S. Ct.) (Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari filed July 8, 2013; petition denied Nov. 18, 2013); *Smith v. Obama*, Civ. No. 2:13-00257 (D. Idaho) (complaint filed June 12, 2013); *First Unitarian Church of Los Angeles v. NSA*, Civ. No. 13-3287 (N.D. Cal.) (complaint filed July 16, 2013).

[3] Plaintiffs' complaints reflect their intention to bring both suits as class actions on behalf of themselves and "all other similarly situated consumers, users, and U.S. citizens who are customers and users of," Second Am. Compl. ("*Klayman I*") ¶ 1, or "who are subscribers, users, customers, and otherwise avail themselves to," Am. Compl. ("*Klayman II*") ¶ 1, the telecommunications and internet companies named in the complaints. Plaintiffs have not yet, however, moved to certify a class in either case and in fact have moved for extensions of time to file a motion for class certification four times in each case. *See* Motion for Extension of Time to Certify Class Action (*Klayman I*) [Dkt. ## 7, 14, 27, 40]; (*Klayman II*) [Dkt. ## 6, 11, 23, 33].

300

call records under the mass call surveillance program; (ii) requires [d]efendants to destroy all of [p]laintiffs' call records already collected under the program; and (iii) prohibits [d]efendants from querying metadata obtained through the program using any phone number or other identifier associated with [p]laintiffs . . . and such other relief as may be found just and proper." Pls.' Mot. for Prelim. Inj. (*Klayman I*) [Dkt. # 13]; Pls.' Mot. for Prelim. Inj. (*Klayman II*) [Dkt. # 10]; *see also* Pls.' Mem. P. & A. in Supp. of Mot. for Prelim. Inj. (*Klayman I*) ("Pls.' Mem.") [Dkt. # 13-1], at 30-31.[4] In light of how plaintiffs have crafted their requested relief, the Court construes the motions as requesting a preliminary injunction (1) only as against the federal government defendants, and (2) only with regard to the government's bulk collection and querying of phone record metadata. Further, between the two cases, plaintiffs have alleged with sufficient particularity that only two of the five named plaintiffs, Larry Klayman and Charles Strange, are telephone service subscribers.[5] Accordingly, for purposes of

[4] Unless otherwise indicated, all citations to "Pls.' Mem." and other docket items hereinafter shall refer to the filings made in *Klayman I*.

[5] In *Klayman I*, plaintiffs Larry Klayman and Charles Strange have submitted affidavits stating they are subscribers of Verizon Wireless for cellular phone service, *see* Aff. of Larry Klayman ("Klayman Aff.") [Dkt. # 13-2], at ¶ 3; Suppl. Aff. of Larry Klayman ("Klayman Suppl. Aff.") [Dkt. # 31-2], at ¶ 3; Aff. of Charles Strange ("Strange Aff.") [Dkt. # 13-3], at ¶ 2, but neither the complaint nor the motion affirmatively alleges that Mary Ann Strange is a subscriber of Verizon Wireless or any other phone service, *see* Second Am. Compl. ¶ 10 (describing plaintiff Mary Ann Strange). And in *Klayman II*, where the complaint and motion raise claims regarding the government's collection and analysis of both phone and internet records, the plaintiffs neither specifically allege, nor submit any affidavits stating, that any of them individually is a subscriber of either of the two named telephone company defendants, AT&T and Sprint, *for telephone services*. *See* Aff. of Larry Klayman (*Klayman II*) [Dkt. # 10-2], at ¶ 3 ("I am also a user of internet services by . . . AT&T . . . ."); Suppl. Aff. of Larry Klayman (*Klayman II*) [Dkt. # 26-2], at ¶ 3 (same); Aff. of Charles Strange (*Klayman II*) [Dkt. # 10-3], at ¶ 3 ("I am also a user of internet services by . . . AT&T . . . ."); Am. Compl. ¶ 14 ("Plaintiff Garrison . . . is a consumer and user of Facebook, Google, YouTube, and Microsoft products."). *Compare* Am. Compl.

resolving these two motions, the Court's discussion of relevant facts, statutory background, and legal issues will be circumscribed to those defendants (hereinafter "the Government"), those two plaintiffs (hereinafter "plaintiffs"), and those claims.[6]

(*Klayman II*) ¶ 13 ("Plaintiff Ferrari . . . is a subscriber, consumer, and user of *Sprint*, Google/Gmail, Yahoo!, and Apple. As a prominent private investigator, Ferrari regularly communicates, both telephonically and electronically . . . ." (emphasis added)), *with* Pls.' Mem. (*Klayman II*) [Dkt. # 10-1], at 18 ("Defendants have indisputably also provided the NSA with intrusive and warrantless access to the *internet records* of Plaintiffs Michael Ferrari and Matthew Garrison" (emphasis added)).

[6] *Klayman I* concerns only the collection and analysis of phone record data, and only with respect to private defendant Verizon Communications. *Klayman II*, by contrast, appears to concern the collection and analysis of both phone and internet record data, and includes both phone companies and internet companies as private defendants. In the latter case, Plaintiffs' Motion for Preliminary Injunction [Dkt. # 10] and their Memorandum of Points and Authorities in Support [Dkt. # 10-1] suffer from some confusion as a result of its larger scope. On the face of the Motion itself [Dkt. # 10] and their Proposed Order [Dkt. # 10-4], plaintiffs request relief that is identical to that requested in the motion in *Klayman I*—i.e., relief concerning only the collection and querying of phone record data. Throughout the memorandum in support [Dkt. # 10-1], however, plaintiffs intermingle claims regarding the surveillance of phone and internet data, and then in conclusion request relief arguably concerning only internet data. *See* Pls.' Mem. P. & A. Supp. Mot. Prelim. Inj. (*Klayman II*) [Dkt. # 10-1], at 4, 32 (requesting an injunction that, in part, "bar[s] Defendants from collecting records pertaining to Plaintiffs' online communications and internet activities").

To the extent plaintiffs are, in fact, requesting preliminary injunctive relief regarding any alleged internet data surveillance activity, the Court need not address those claims for two reasons. First, the Government has represented that any bulk collection of internet *metadata* pursuant to Section 215 (50 U.S.C. § 1861) was discontinued in 2011, *see* Govt. Defs.' Opp'n to Pls.' Mot. for Prelim. Inj. ("Govt.'s Opp'n") [Dkt. # 25], at 15-16, 44-45; Ex. J to Decl. of James J. Gilligan ("Gilligan Decl.") [Dkt. # 25-11] (Letter from James R. Clapper to the Sen. Ron Wyden (July 25, 2013)), and therefore there is no possible ongoing harm that could be remedied by injunctive relief. Second, to the extent plaintiffs challenge the Government's targeted collection of internet data *content* pursuant to Section 702 (50 U.S.C. § 1881a) under the so-called "PRISM" program, which targets non-U.S. persons located outside the U.S., plaintiffs have not alleged sufficient facts to show that the NSA has targeted any of their communications. *See* Govt.'s Opp'n at 21-22, 44. Accordingly, plaintiffs lack standing, as squarely dictated by the Supreme Court's recent decision in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), which concerns the same statutory provision. In *Clapper*, the Court held that respondents, whose work purportedly involved engaging in phone and internet contact with persons located abroad, lacked standing to challenge Section 702 because it was speculative whether the government would seek to target, target, and actually acquire their communications. *See Clapper*, 133. S. Ct. at 1148-50 ("[R]espondents' speculative chain of possibilities does not

For the reasons discussed below, the Court first finds that it lacks jurisdiction to hear plaintiffs' Administrative Procedure Act ("APA") claim that the Government has exceeded its statutory authority under the Foreign Intelligence Surveillance Act ("FISA"). Next, the Court finds that it does, however, have the authority to evaluate plaintiffs' constitutional challenges to the NSA's conduct, notwithstanding the fact that it was done pursuant to orders issued by the Foreign Intelligence Surveillance Court ("FISC"). And after careful consideration of the parties' pleadings and supplemental pleadings, the representations made on the record at the November 18, 2013 hearing regarding these two motions, and the applicable law, the Court concludes that plaintiffs have standing to challenge the constitutionality of the Government's bulk collection and querying of phone record metadata, that they have demonstrated a substantial likelihood of success on the merits of their Fourth Amendment claim, and that they will suffer irreparable harm absent preliminary injunctive relief.[7] Accordingly, the Court will GRANT, in part, the Motion for Preliminary Injunction in *Klayman I* (with respect to

---

establish that injury based on potential future surveillance is certainly impending or is fairly traceable to § 1881a."). So too for plaintiffs here. (In fact, plaintiffs here have not even alleged that they communicate with anyone outside the United States at all, so their claims under Section 702 are even less colorable than those of the plaintiffs in *Clapper*.)

[7] Because I ultimately find that plaintiffs have made a sufficient showing to merit injunctive relief on their Fourth Amendment claim, I do not reach their other constitutional claims under the First and Fifth Amendments. *See Seven-Sky v. Holder*, 661 F.3d 1, 46 (D.C. Cir. 2011) (noting "the bedrock principle of judicial restraint that courts avoid prematurely or unnecessarily deciding constitutional questions"), *abrogated by Nat'l Fed'n of Indep. Bus. v. Sebelius*, 132 S. Ct. 2566 (2012); *see also Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 450 (2008) (noting "the fundamental principle of judicial restraint that courts should neither anticipate a question of constitutional law in advance of the necessity of deciding it nor formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied" (citations and internal quotation marks omitted)).

Larry Klayman and Charles Strange only), and DENY the Motion for Preliminary Injunction in *Klayman II*. However, in view of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will STAY my order pending appeal.

BACKGROUND

On June 5, 2013, the British newspaper *The Guardian* reported the first of several "leaks" of classified material from Edward Snowden, a former NSA contract employee, which have revealed—and continue to reveal—multiple U.S. government intelligence collection and surveillance programs. *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, GUARDIAN (London), June 5, 2013.[8] That initial media report disclosed a FISC order dated April 25, 2013, compelling Verizon Business Network Services to produce to the NSA on "an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Secondary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services*, No. BR 13-80 at 2 (FISC Apr. 25, 2013) (attached as Ex. F to Gilligan Decl.) [Dkt. # 25-7] ("Apr. 25, 2013 Secondary Order"). According to the news article, this order "show[ed] . . . that under the Obama administration the communication records of millions of US

[8] *Available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing." Greenwald, *supra*. In response to this disclosure, the Government confirmed the authenticity of the April 25, 2013 FISC Order, and, in this litigation and in certain public statements, acknowledged the existence of a "program" under which "the FBI obtains orders from the FISC pursuant to Section 215 [of the USA PATRIOT Act] directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of 'call detail records.'" Govt.'s Opp'n at 8.[9] Follow-on media reports revealed other Government surveillance programs, including the Government's collection of internet data pursuant to a program called "PRISM." *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, GUARDIAN (London), June 6, 2013.[10]

---

[9] Although aspects of the program remain classified, including which other telecommunications service providers besides Verizon Business Network Services are involved, the Government has declassified and made available to the public certain facts about the program. *See* Office of the Dir. of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosure of Classified Information* (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information; Office of the Dir. of Nat'l Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)* (Aug. 21, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa; Office of the Dir. of Nat'l Intelligence, *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)* (Sept. 10, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document; Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act (Aug. 9, 2013), *available at* . http://apps.washingtonpost.com/g/page/politics/obama-administration-white-paper-on-nsa-surveillance-oversight/388/.

[10] *Available at* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Soon after the first public revelations in the news media, plaintiffs filed their complaints in these two cases on June 6, 2013 (*Klayman I*) and June 12, 2013 (*Klayman II*), alleging that the Government, with the participation of private companies, is conducting "a secret and illegal government scheme to intercept and analyze vast quantities of domestic telephonic communications," Second Am. Compl. ¶ 2 (*Klayman I*), and "of communications from the Internet and electronic service providers," Am. Compl. ¶ 2 (*Klayman II*). Plaintiffs in *Klayman I*—attorney Larry Klayman, founder of Freedom Watch, a public interest organization, and Charles Strange, the father of Michael Strange, a cryptologist technician for the NSA and support personnel for Navy SEAL Team VI who was killed in Afghanistan when his helicopter was shot down in 2011—assert that they are subscribers of Verizon Wireless and bring suit against the NSA, the Department of Justice ("DOJ"), and several executive officials (President Barack H. Obama, Attorney General Eric H. Holder, Jr., General Keith B. Alexander, Director of the NSA, and U.S. District Judge Roger Vinson), as well as Verizon Communications and its chief executive officer. Second Am. Compl. ¶¶ 9-19; Klayman Aff. ¶ 3; Strange Aff. ¶ 2. And plaintiffs in *Klayman II*—Mr. Klayman and Mr. Strange again, along with two private investigators, Michael Ferrari and Matthew Garrison—bring suit against the same Government defendants, as well as Facebook, Yahoo!, Google, Microsoft, YouTube, AOL, PalTalk, Skype, Sprint, AT&T, and Apple, asserting that plaintiffs are "subscribers, users, customers, and otherwise avail themselves to" these named internet and/or telephone service provider companies. Am. Compl. ¶¶ 1, 11-14;

306

Klayman Aff. ¶ 3; Klayman Suppl. Aff. ¶ 3; Strange Aff. ¶ 3.[11] Specifically, plaintiffs allege that the Government has violated their individual rights under the First, Fourth, and Fifth Amendments of the Constitution and has violated the Administrative Procedure Act ("APA") by exceeding its statutory authority under FISA.[12] Second Am. Compl. ¶¶ 1-8, 49-99.

I. Statutory Background

A. FISA and Section 215 of the USA PATRIOT Act (50 U.S.C. § 1861)

In 1978, Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 *et seq.* ("FISA"), "to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013). Against the backdrop of findings by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the "Church Committee") that the executive branch had, for decades, engaged in warrantless domestic intelligence-gathering activities that had illegally infringed the Fourth Amendment rights of American citizens, Congress passed FISA "in large measure [as] a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused." S. Rep. No. 95-604, at 7. In the view of the Senate Judiciary Committee, the act went "a long way in striking a fair and just balance between protection of national security and protection of personal liberties." *Id.* at 7.

---

[11] *See supra*, notes 5, 6.

[12] Plaintiffs also allege certain statutory violations by the private company defendants, Second Am. Compl. ¶¶ 81-95, which are not at issue for purposes of the Preliminary Injunction Motions, as well as common law privacy tort claims, Second Am. Compl. ¶¶ 70-80.

FISA created a procedure for the Government to obtain ex parte judicial orders authorizing domestic electronic surveillance upon a showing that, *inter alia*, the target of the surveillance was a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1804(a)(3), 1805(a)(2). In enacting FISA, Congress also created two new Article III courts—the Foreign Intelligence Surveillance Court ("FISC"), composed of eleven U.S. district judges, "which shall have jurisdiction to hear applications for and grant orders approving" such surveillance, § 1803(a)(1), and the FISC Court of Review, composed of three U.S. district or court of appeals judges, "which shall have jurisdiction to review the denial of any application made under [FISA]," § 1803(b).[13]

In addition to authorizing wiretaps, §§ 1801-1812, FISA was subsequently amended to add provisions enabling the Government to obtain ex parte orders authorizing physical searches, §§ 1821-1829, as well as pen registers and trap-and-trace devices, §§ 1841-1846. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807(a)(3), 108 Stat. 3423; Intelligence Authorization Act for Fiscal Year 1999,

[13] The eleven U.S. district judges are appointed by the Chief Justice of the United States to serve on the FISC for a term of seven years each. 50 U.S.C. § 1803(a)(1), (d). They are drawn from at least seven of the twelve judicial circuits in the United States, and at least three of the judges must reside within twenty miles of the District of Columbia. § 1803(a)(1). For these eleven district judges who comprise the FISC at any one time, their service on the FISC is *in addition to*, not in lieu of, their normal judicial duties in the districts in which they have been appointed. *See* Theodore W. Ruger, *Chief Justice Rehquist's Appointments to the FISA Court: An Empirical Perspective*, 101 NW. U. L. REV. 239, 244 (2007) ("Service on the FISA Court is a part-time position. The judges rotate through the court periodically and maintain regular district court caseloads in their home courts."). Accordingly, service on the FISC is, at best, a part-time assignment that occupies a relatively small part of each judge's annual judicial duties. Further, as a result of the requirement that at least three judges reside within twenty miles of the nation's capital, a disproportionate number of the FISC judges are drawn from the district courts of the District of Columbia and the Eastern District of Virginia, *see id.* at 258 (Appendix) (listing Chief Justice Rehnquist's twenty-five appointments to the FISC, six of which came from the D.D.C. and E.D. Va.).

Pub. L. No. 105-272, § 601(2), 112 Stat. 2396 ("1999 Act"). In 1998, Congress added a "business records" provision to FISA. *See* 1999 Act § 602. Under that provision, the FBI was permitted to apply for an ex parte order authorizing specified entities, such as common carriers, to release to the FBI copies of business records upon a showing in the FBI's application that "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." 50 U.S.C. § 1862(b)(2)(B) (2000).

Following the September 11, 2001 terrorist attacks, Congress passed the USA PATRIOT Act, which made changes to FISA and several other laws. Pub. L. No. 107-56, 115 Stat. 272 (2001). Section 215 of the PATRIOT Act replaced FISA's business-records provision with a more expansive "tangible things" provision. Codified at 50 U.S.C. § 1861, it authorizes the FBI to apply "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." § 1861(a)(1). While this provision originally required that the FBI's application "shall specify that the records concerned are sought for" such an investigation, § 1861(b)(2) (Supp. I 2001), Congress amended the statute in 2006 to provide that the FBI's application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." §

1861(b)(2)(A); *see* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 ("USA PATRIOT Improvement and Reauthorization Act").

Section 1861 also imposes other requirements on the FBI when seeking to use this authority. For example, the investigation pursuant to which the request is made must be authorized and conducted under guidelines approved by the Attorney General under Executive Order No. 12,333 (or a successor thereto). 50 U.S.C. § 1861(a)(2)(A), (b)(2)(A). And the FBI's application must "enumerat[e] . . . minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination by the [FBI] of any tangible things to be made available to the [FBI] based on the order requested." § 1861(b)(2)(B). The statute defines "minimization procedures" as, in relevant part, "specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting [U.S.] persons consistent with the need of the [U.S.] to obtain, produce, and disseminate foreign intelligence information." § 1861(g)(2). If the FISC judge finds that the FBI's application meets these requirements, he "shall enter an ex parte order as requested, or as modified, approving the release of tangible things" (hereinafter, "production order"). § 1861(c)(1); *see also* § 1861(f)(1)(A) ("the term 'production order' means an order to produce any tangible thing under this section").

Under Section 1861's "use" provision, information that the FBI acquires through such a production order "concerning any [U.S.] person may be used and disclosed by

Federal officers and employees without the consent of the [U.S.] person only in accordance with the minimization procedures adopted" by the Attorney General and approved by the FISC. § 1861(h). Meanwhile, recipients of Section 1861 production orders are obligated not to disclose the existence of the orders, with limited exceptions. § 1861(d)(1).

B. Judicial Review by the FISC

While the recipient of a production order must keep it secret, Section 1861 does provide the recipient—but only the recipient—a right of judicial review of the order before the FISC pursuant to specific procedures. Prior to 2006, recipients of Section 1861 production orders had no express right to judicial review of those orders, but Congress added such a provision when it reauthorized the PATRIOT Act that year. *See* USA PATRIOT Improvement and Reauthorization Act § 106(f); 1 D. KRIS & J. WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 19:7 (2d ed. 2012) ("Kris & Wilson") ("Prior to the Reauthorization Act in 2006, FISA did not allow for two-party litigation before the FISC.").

Under Section 1861, "[a] person receiving a production order may challenge the legality of that order by filing a petition with the [petition review pool of FISC judges]." 50 U.S.C. § 1861(f)(2)(A)(i); *see* § 1803(e)(1).[14] The FISC review pool judge considering the petition may grant the petition "only if the judge finds that [the] order

[14] The three judges who reside within twenty miles of the District of Columbia comprise the petition review pool (unless all three are unavailable, in which case other FISC judges may be designated). § 1803(e)(1). In addition to reviewing petitions to review Section 1861 production orders pursuant to § 1861(f), the review pool also has jurisdiction to review petitions filed pursuant to § 1881a(h)(4). *Id.*

does not meet the requirements of [Section 1861] or is otherwise unlawful." § 1861(f)(2)(B). Once the FISC review pool judge rules on the petition, either the Government or the recipient of the production order may seek an en banc hearing before the full FISC, § 1803(a)(2)(A), or may appeal the decision by filing a petition for review with the FISC Court of Review, § 1861(f)(3). Finally, after the FISC Court of Review renders a written decision, either the Government or the recipient of the production order may then appeal this decision to the Supreme Court on petition for writ of certiorari. §§ 1861(f)(3), 1803(b). A production order "not explicitly modified or set aside consistent with [Section 1861(f)] shall remain in full effect." § 1861(f)(2)(D).

Consistent with other confidentiality provisions of FISA, Section 1861 provides that "[a]ll petitions under this subsection shall be filed under seal," § 1861(f)(5), and the "record of proceedings . . . shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence," § 1861(f)(4). *See also* § 1803(c).

II. Collection of Bulk Telephony Metadata Pursuant to Section 1861

To say the least, plaintiffs and the Government have portrayed the scope of the Government's surveillance activities very differently.[15] For purposes of resolving these preliminary injunction motions, however, as will be made clear in the discussion below, it

[15] In addition to alleging that the NSA has "direct access" to Verizon's databases, Second Am. Compl. ¶ 7, and is collecting location information as part of "call detail records," Pls. Mem. at 10, Mr. Klayman and Mr. Strange also suggest that they are "prime target[s]" of the Government due to their public advocacy and claim that the Government is behind alleged inexplicable text messages being sent from and received on their phones, Pls.' Mem. at 13-16; Klayman Aff. ¶ 11; Strange Aff. ¶¶ 12-17.

will suffice to accept the Government's description of the phone metadata collection and querying program. *Cf. Cobell v. Norton*, 391 F.3d 251, 261 (D.C. Cir. 2004) (evidentiary hearing on preliminary injunction is necessary only if the court must make credibility determinations to resolve key factual disputes in favor of the *moving party*).

In broad overview, the Government has developed a "counterterrorism program" under Section 1861 in which it collect, compiles, retains, and analyzes certain telephone records, which it characterizes as "business records" created by certain telecommunications companies (the "Bulk Telephony Metadata Program"). The records collected under this program consist of "metadata," such as information about what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted. Decl. of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation ("Holley Decl.") [Dkt. # 25-5], at ¶ 5; Decl. of Teresa H. Shea, Signals Intelligence Director, National Security Agency ("Shea Decl.") [Dkt. # 25-4], at ¶ 7; Primary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things From [Redacted]*, No. BR 13-158 at 3 n.1 (FISC Oct. 11, 2013) (attached as Ex. B to Gilligan Decl.) [Dkt. # 25-3] ("Oct. 11, 2013 Primary Order").[16] According to the representations made by the Government, the metadata records collected under the program do *not* include *any* information about the content of those

[16] Oct. 11, 2013 Primary Order at 3 n.1 ("For purposes of this Order 'telephony metadata' includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.").

313

calls, or the names, addresses, or financial information of any party to the calls. Holley Decl. ¶¶ 5, 7; Shea Decl. ¶ 15; Oct. 11, 2013 Primary Order at 3 n.1.[17] Through targeted computerized searches of those metadata records, the NSA tries to discern connections between terrorist organizations and previously unknown terrorist operatives located in the United States. Holley Decl. ¶ 5; Shea Decl. ¶¶ 8-10, 44.

The Government has conducted the Bulk Telephony Metadata Program for more than seven years. Beginning in May 2006 and continuing through the present,[18] the FBI has obtained production orders from the FISC under Section 1861 directing certain telecommunications companies to produce, on an ongoing daily basis, these telephony metadata records, Holley Decl. ¶ 6; Shea Decl. ¶ 13, which the companies create and maintain as part of their business of providing telecommunications services to customers, Holley Decl. ¶ 10; Shea Decl. ¶ 18. The NSA then consolidates the metadata records provided by different telecommunications companies into one database, Shea Decl. ¶ 23, and under the FISC's orders, the NSA may retain the records for up to five years, *id.* ¶

[17] Plaintiffs have alleged that the Government has also collected location information for cell phones. Second Am. Comp. ¶ 28; Pls.' Mem. at 10-11. While more recent FISC opinions expressly state that cell-site location information is not covered by Section 1861 production orders, *see, e.g.*, Oct. 11, 2013 Primary Order at 3 n.1, the Government has *not* affirmatively represented to this Court that the NSA has *not*, at any point in the history of the Bulk Telephony Metadata Program, collected location information (in one technical format or another) about cell phones. *See, e.g.*, Govt.'s Opp'n at 9 (defining telephony metadata and noting what is not included); Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 06-05 at 2 (FISC May 24, 2006), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document (defining telephony metadata and noting what is not included, but *not* expressly stating that the order does *not* authorize the production of cell-site location information).

[18] The most recent FISC order authorizing the Bulk Telephony Metadata Program that the Government has disclosed (in redacted form, directed to an unknown recipient) expires on January 3, 2014. *See* Oct. 11, 2013 Primary Order at 17.

30; *see* Oct. 11, 2013 Primary Order at 14. According to Government officials, this aggregation of records into a single database creates "an historical repository that permits retrospective analysis," Govt.'s Opp'n at 12, enabling NSA analysts to draw connections, across telecommunications service providers, between numbers reasonably suspected to be associated with terrorist activity and with other, unknown numbers. Holley Decl. ¶¶ 5, 8; Shea Decl. ¶¶ 46, 60.

The FISC orders governing the Bulk Telephony Metadata Program specifically provide that the metadata records may be accessed only for counterterrorism purposes (and technical database maintenance). Holley Decl. ¶ 8; Shea Decl. ¶ 30. Specifically, NSA intelligence analysts, *without seeking the approval of a judicial officer*, may access the records to obtain foreign intelligence information only through "queries" of the records performed using "identifiers," such as telephone numbers, associated with terrorist activity.[19] An "identifier" (i.e., selection term, or search term) used to start a query of the database is called a "seed," and "seeds" must be approved by one of twenty-two designated officials in the NSA's Homeland Security Analysis Center or other parts of the NSA's Signals Intelligence Directorate. Shea Decl. ¶¶ 19, 31. Such approval may be given only upon a determination by one of those designated officials that there exist facts giving rise to a "reasonable, articulable suspicion" ("RAS") that the selection term

[19] In her declaration, Teresa H. Shea, Director of the Signals Intelligence Directorate at the NSA, states that "queries," or "term searches," of the metadata database are conducted "using metadata 'identifiers,' *e.g., telephone numbers*, that are associated with a foreign terrorist organization." Shea Decl. ¶ 19 (emphasis added). If a telephone number is only an *example* of an identifier that may be used as a search term, it is not clear what other "identifiers" may be used to query the database, and the Government has not elaborated. *See, e.g.*, Oct. 11, 2013 Primary Order at 5 n.4, 7-10 (redacting text that appears to discuss "selection terms").

to be queried is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC. Holley Decl. ¶¶ 15-16.[20] In 2012, for example, fewer than 300 unique identifiers met this RAS standard and were used as "seeds" to query the metadata, but "the number of unique identifiers has varied over the years." Shea Decl. ¶ 24.

When an NSA intelligence analyst runs a query using a "seed," the minimization procedures provide that query results are limited to records of communications within three "hops" from the seed. *Id.* ¶ 22. The query results thus will include only identifiers and their associated metadata having a direct contact with the seed (the first "hop"), identifiers and associated metadata having a direct contact with first "hop" identifiers (the second "hop"), and identifiers and associated metadata having a direct contact with second "hop" identifiers (the third "hop"). *Id.* ¶ 22; Govt.'s Opp'n at 11. In plain English, this means that if a search starts with telephone number (123) 456-7890 as the "seed," the first hop will include all the phone numbers that (123) 456-7890 has called or received calls from in the last five years (say, 100 numbers), the second hop will include all the phone numbers that each of *those* 100 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 100 "first hop" numbers, or 10,000 total), and the third hop will include all the phone numbers that each of *those* 10,000 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 10,000 "second hop" numbers, or 1,000,000 total). *See* Shea Decl. ¶

[20] A determination that a selection term meets the RAS standard remains effective for 180 days for any selection term reasonably believed to be used by a U.S. person, and for one year for all other selection terms. *See* Oct. 11, 2013 Primary Order at 10.

25 n.1. The actual number of telephone numbers and their associated metadata captured in any given query varies, of course, but in the absence of any specific representations from the Government about typical query results, it is likely that the quantity of phone numbers captured in any given query would be very large.[21]

[21] After stating that fewer than 300 unique identifiers met the RAS standard and were used as "seeds" to query the metadata in 2012, Ms. Shea notes that "[b]ecause the same seed identifier can be queried more than once over time, can generate multiple responsive records, and can be used to obtain contact numbers up to three 'hops' from the seed identifier, the number of metadata records responsive to such queries is *substantially larger than 300, but is still a very small percentage of the total volume of metadata records*." Shea Decl. ¶ 24 (emphasis added). The first part of this assertion is a glaring understatement, while the second part is virtually meaningless when placed in context. First, as the sample numbers I have used in the text above demonstrate, it is possible to arrive at a query result in the millions within three hops while using even conservative numbers—needless to say, this is "substantially larger than 300." After all, even if the average person in the United States does not call or receive calls from 100 unique phone numbers in one year, what about over a five-year period? And second, it belabors the obvious to note that even a few million phone numbers is "a very small percentage of the total volume of metadata records" if the Government has collected metadata records on hundreds of millions of phone numbers.

But it's also easy to imagine the spiderweb-like reach of the three-hop search growing exponentially and capturing even higher numbers of phone numbers. Suppose, for instance, that there is a person living in New York City who has a phone number that meets the RAS standard and is approved as a "seed." And suppose this person, who may or may not actually be associated with any terrorist organization, calls or receives calls from 100 unique numbers, as in my example. But now suppose that one of the numbers he calls is his neighborhood Domino's Pizza shop. The Court won't hazard a guess as to how many different phone numbers might dial a given Domino's Pizza outlet in New York City in a five-year period, but to take a page from the Government's book of understatement, it's "substantially larger" than the 100 in the second hop of my example, and would therefore most likely result in exponential growth in the scope of the query and lead to millions of records being captured by the third hop. (I recognize that some minimization procedures described in recent FISC orders permitting technical personnel to access the metadata database to "defeat [] high volume and other unwanted [] metadata," Oct. 11, 2013 Primary Order at 6, may, in practice, reduce the likelihood of my Domino's hypothetical example occurring. But, of course, that does not change the baseline fact that, by the terms of the FISC's orders, the NSA is permitted to run queries capturing up to three hops that can conceivably capture millions of Americans' phone records. Further, these queries using non-RAS-approved selection terms, which are permitted to make the database "usable for intelligence analysis," *id.* at 5, may very well themselves involve searching across millions of records.)

Once a query is conducted and it returns a universe of responsive records (i.e., a universe limited to records of communications within three hops from the seed), trained NSA analysts may then perform new searches and otherwise perform intelligence analysis *within* that universe of data without using RAS-approved search terms. *See* Shea Decl. ¶ 26 (NSA analysts may "chain contacts within the query results themselves"); Oct. 11, 2013 Primary Order.[22] According to the Government, following the "chains of communication"—which, for chains that cross different communications networks, is only possible if the metadata is aggregated—allows the analyst to discover information that may not be readily ascertainable through other, targeted intelligence-gathering techniques. Shea Decl. ¶ 46. For example, the query might reveal that a seed telephone number has been in contact with a previously unknown U.S. telephone number—i.e., on the first hop. *See id.* ¶ 58. And from there, "contact-chaining" out to the second and third hops to examine the contacts made by that telephone number may reveal a contact with other telephone numbers already known to the Government to be associated with a foreign terrorist organization. *Id.* ¶¶ 47, 62. In short, the Bulk Telephony Metadata Program is meant to detect: (1) domestic U.S. phone numbers calling *outside* of the U.S. to foreign phone numbers associated with terrorist groups; (2) foreign phone numbers

[22] Under the terms of the most recent FISC production order available, "[q]ueries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below. This automated query process queries the collected BR metadata (in a 'collection store') with RAS-approved selection terms and returns the hop-limited results from those queries to a 'corporate store.' The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms." Oct. 11, 2013 Primary Order at 11 (footnote omitted). This "automated query process" was first approved by the FISC in a November 8, 2012 order. *Id.* at 11 n.11.

associated with terrorist groups calling *into* the U.S. to U.S. phone numbers; and (3) "possible terrorist-related communications" between U.S. phone numbers *inside* the U.S. *See id.* ¶ 44.

Since the program began in May 2006, the FISC has repeatedly approved applications under Section 1861 and issued orders directing telecommunications service providers to produce records in connection with the Bulk Telephony Metadata Program. Shea Decl. ¶¶ 13-14. Through October 2013, fifteen different FISC judges have issued thirty-five orders authorizing the program. Govt.'s Opp'n at 9; *see also* Shea Decl. ¶¶ 13-14; Holley Decl. ¶ 6. Under those orders, the Government must periodically seek renewal of the authority to collect telephony records (typically every ninety days). Shea Decl. ¶ 14. The Government has nonetheless acknowledged, as it must, that failures to comply with the minimization procedures set forth in the orders have occurred. For instance, in January 2009, the Government reported to the FISC that the NSA had improperly used an "alert list" of identifiers to search the bulk telephony metadata, which was composed of identifiers that had *not* been approved under the RAS standard. *Id.* ¶ 37; Order, *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, 2009 WL 9150913, at *2 (FISC Mar. 2, 2009) ("Mar. 2, 2009 Order"). After reviewing the Government's reports on its noncompliance, Judge Reggie Walton of the FISC concluded that the NSA had engaged in "systematic noncompliance" with FISC-ordered minimization procedures over the preceding three years, since the inception of the Bulk Telephony Metadata Program, and had also repeatedly made misrepresentations and inaccurate statements about the program to the FISC judges. Mar. 2, 2009 Order, 2009

WL 9150913, at *2-5.[23] As a consequence, Judge Walton concluded that he had no confidence that the Government was doing its utmost to comply with the court's orders, and ordered the NSA to seek FISC approval on a *case-by-case basis* before conducting any further queries of the bulk telephony metadata collected pursuant to Section 1861 orders. *Id.* at *9; Shea Decl. ¶¶ 38-39. This approval procedure remained in place from March 2009 to September 2009. Shea Decl. ¶¶ 38-39.

Notwithstanding this six-month "sanction" imposed by Judge Walton, the Government apparently has had further compliance problems relating to its collection programs in subsequent years. In October 2011, the Presiding Judge of the FISC, Judge John Bates, found that the Government had misrepresented the scope of its targeting of certain internet communications pursuant to 50 U.S.C. § 1881a (i.e., a different collection program than the Bulk Telephony Metadata Program at issue here). Referencing the 2009 compliance issue regarding the NSA's use of unauthorized identifiers to query the metadata in the Bulk Telephony Metadata Program, Judge Bates wrote: "the Court is

[23] Judge Walton noted that, "since the earliest days of the FISC-authorized collection of call-detail records by the NSA, the NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non-RAS-approved telephone identifiers on its alert list against the BR metadata in order to identify any matches. Such access was prohibited by the governing minimization procedures under each of the relevant Court orders." Mar. 2, 2009 Order, 2009 WL 9150913, at *2. He went on to conclude: "In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively." *Id.* at *5.

troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program." Mem. Op., *[Redacted]*, No. [redacted], at 16 n.14 (FISC Oct. 3, 2011).[24] Both Judge Walton's and Judge Bates's opinions were only recently declassified by the Government in response to the Congressional and public reaction to the Snowden leaks.[25]

ANALYSIS

I will address plaintiffs' statutory claim under the APA before I turn to their constitutional claim under the Fourth Amendment.

I. Statutory Claim Under the APA

Invoking this Court's federal question jurisdiction under 28 U.S.C. §·1331, plaintiffs allege that the Government's phone metadata collection and querying program exceeds the statutory authority granted by FISA's "tangible things" provision, 50 U.S.C. § 1861, and thereby violates the Administrative Procedure Act ("APA"), 5 U.S.C. § 706.

---

[24] *Available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa. Whatever the second "substantial misrepresentation" was, the Government appears to have redacted it from the footnote in that opinion.

[25] *See* Office of the Dir. of Nat'l Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)* (Aug. 21, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa; Office of the Dir. of Nat'l Intelligence, *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)* (Sept. 10, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document.

See Second Am. Compl. ¶¶ 96-99; Pls.' Mem. at 2, 17-19; Pls.' Reply in Supp. of Mots. for Prelim. Inj. ("Pls.' Reply") [Dkt. # 31], at 5-11. In particular, plaintiffs argue that the bulk records obtained under the Bulk Telephony Metadata Program are not "relevant" to authorized national security investigations, *see* 50 U.S.C. § 1861(b)(2)(A), and that the FISC may not prospectively order telecommunications service providers to produce records that do not yet exist. *See* Pls.' Mem. at 17-19; Pls.' Reply at 5-11. In response, the Government argues that this Court lacks subject matter jurisdiction over this statutory claim because Congress impliedly precluded APA review of such claims. Government Defs.' Supplemental Br. in Opposition to Pls.' Mots. Prelim. Inj. ("Govt.'s Suppl. Br.") [Dkt. # 43], at 2. For the following reasons, I agree with the Government that I am precluded from reviewing plaintiffs' APA claim.

The APA "establishes a cause of action for those 'suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action.'" *Koretoff v. Vilsack*, 614 F.3d 532, 536 (D.C. Cir. 2010) (quoting 5 U.S.C. § 702). In particular, the APA permits such aggrieved persons to bring suit against the United States and its officers for "relief other than money damages," 5 U.S.C. § 702, such as the injunctive relief plaintiffs seek here. This general waiver of sovereign immunity does not apply, however, "if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." *Id.* Similarly the APA's "basic presumption of judicial review [of agency action]," *Abbott Labs v. Gardner*, 387 U.S. 136, 140 (1967), does not apply "to the extent that . . . statutes preclude judicial review," 5 U.S.C. § 701(a)(1). Accordingly, "[t]he presumption favoring judicial review of administrative action is just

that—a presumption," *Block v. Community Nutrition Inst.*, 467 U.S. 340, 349 (1984), and it may be overcome "whenever the congressional intent to preclude judicial review is 'fairly discernible in the statutory scheme.'" *Id.* at 351. Assessing "[w]hether a statute precludes judicial review of agency action . . . is a question of congressional intent, which is determined from the statute's 'express language,' as well as 'from the structure of the statutory scheme, its objectives, its legislative history, and the nature of the administrative action involved.'" *Koretoff*, 614 F.3d at 536 (quoting *Block*, 467 U.S. at 345); *see also Thunder Basin Coal Co. v. Reich*, 510 U.S. 200, 207 (1994).

The Government insists that two statutes—50 U.S.C. § 1861, the "tangible things" provision of FISA itself, and 18 U.S.C. § 2712, a provision of the USA PATRIOT Act, codified in the Stored Communications Act—*impliedly* preclude this Court's review of plaintiffs' statutory APA claim. Govt.'s Opp'n at 26-31; Govt.'s Suppl. Br. at 1-4. The text of Section 1861, and the structure and purpose of the FISA statutory scheme, as a whole, do indeed reflect Congress's preclusive intent. Stated simply, Congress created a closed system of judicial review of the government's domestic foreign intelligence-gathering, generally, 50 U.S.C. § 1803, and of Section 1861 production orders, specifically, § 1861(f). This closed system includes no role for third parties, such as plaintiffs here, nor courts besides the FISC, such as this District Court. Congress's preclusive intent is therefore sufficiently clear. How so?

First, and most directly, the text of the applicable provision of FISA itself, Section 1861, evinces Congress's intent to preclude APA claims like those brought by plaintiffs before this Court. Section 1861 expressly provides a right of judicial review of orders to

produce records, but it only extends that right to the *recipients* of such orders, such as telecommunications service providers. *See* 50 U.S.C. § 1861(f). Congress thus did *not* preclude *all* judicial review of Section 1861 production orders, but I, of course, must determine "whether Congress nevertheless foreclosed review to the class to which the [plaintiffs] belon[g]." *Block*, 467 U.S. at 345-46. And "when a statute provides a detailed mechanism for judicial consideration of *particular issues* at the behest of *particular persons*, judicial review of *those issues* at the behest of *other persons* may be found to be impliedly precluded." *Id.* at 349 (emphases added); *see also id.* at 345-48 (holding that the statutory scheme of the Agricultural Marketing Agreement Act ("AMAA"), which expressly provided a mechanism for milk *handlers* to obtain judicial review of milk market orders issued by the Secretary of Agriculture, impliedly precluded review of those orders in suits brought by milk *consumers*). That is exactly the case here. Congress has established a detailed scheme of judicial review of the particular issue of the "legality" of Section 1861 production orders at the behest of only recipients of those orders. 50 U.S.C. §§ 1861(f)(2)(A)(i) ("A person receiving a production order may challenge the *legality* of that order by filing a petition with the [petition review pool of FISC judges]." (emphasis added)), 1861(f)(2)(B) ("A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order *does not meet the requirements of this section or is otherwise unlawful*." (emphasis added)). And that scheme of judicial review places such challenges before the FISC: Section 1861 permits such challenges to be heard only by the petition review pool

of the FISC. *See* § 1861(f)(2)(A)(i); § 1803(e)(1) (the FISC petition review pool "shall have jurisdiction to review petitions filed pursuant to section 1861(f)(1) . . . of this title").

Second, the purpose and legislative history of Section 1861 also support the conclusion that Congress intended to preclude APA claims by third parties. Simply put, Congress did not envision that third parties, such as plaintiffs, would even *know* about the existence of Section 1861 orders, much less challenge their legality under the statute. *See, e.g.*, H.R. Rep. No. 109-174 at 128, 268 (2005). As the Government points out, "Section [1861], like other provisions of FISA, establishes a secret and expeditious process that involves only the Government and the recipient of the order" in order to "promote its effective functioning as a tool for counter-terrorism." Govt.'s Opp'n at 29; *see also* 50 U.S.C. § 1861(d)(1) (recipient of production order may not "disclose to any other person that the [FBI] has sought or obtained" an order under Section 1861); § 1861(f)(5) ("All petitions under this subsection shall be filed under seal."); § 1861(f)(4) ("The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence."). Congress did think about third parties, such as persons whose records would be targeted, when it created a right to judicial review of Section 1861 production orders for recipients, but it recognized that extending a similar right to third parties would make little sense in light of the secrecy of such orders. *See*

H.R. Rep. No. 109-174 at 128, 268; Govt.'s Opp'n at 29 n.14; Govt.'s Suppl. Br. at 3.[26] Congress therefore considered the precise issue of challenges to the legality of Section 1861 orders, and the statute reflects its ultimate conclusions as to who may seek review and in what court. § 1861(f); *see also* H.R. Rep. No. 109-174 at 128-29, 134, 137 (rejecting amendment that would have allowed recipients of Section 1861 orders to bring challenges to such orders in federal district court).

But even setting aside the specific fact that FISA does not contain a judicial review provision for third parties regarding Section 1861 orders, Congress's preclusive intent is all the more evident when one considers, viewing FISA as a whole, that Congress did not contemplate the participation of third parties in the statutory scheme *at all*. *See Ark. Dairy Coop. Ass'n v. Dep't of Agric.*, 573 F.3d 815, 822 (D.C. Cir. 2009) (noting that in reaching its decision in *Block*, "the Supreme Court did not concentrate simply on the presence or absence of an explicit right of appeal [for consumers] in the AMAA, but instead noted that in the 'complex scheme' of the AMAA, there was no provision for consumer participation of any kind.").[27] Indeed, until 2006, FISA did not

[26] Congress has also not provided a suppression remedy for tangible things obtained under Section 1861, in contrast to the "use of information" provisions under nearly every other subchapter of FISA, which contain such a remedy. *Compare* 50 U.S.C. § 1861 *with* §§ 1806(e) (evidence obtained or derived from an electronic surveillance), 1825(f) (evidence obtained or derived from a physical search), 1845(e) (evidence obtained or derived from the use of a pen register or trap and trace device), 1881e (deeming information acquired under the section to be acquired "from an electronic surveillance" for purposes of Section 1806).

[27] In *Arkansas Dairy*, our Circuit Court addressed a suit concerning the AMAA, the same statute at issue in *Block*. The government, relying on *Block*'s holding that milk *consumers* were barred from bringing a claim because the statute did not grant them an express right to judicial review, argued that milk *producers* likewise could not bring an action because the AMAA did not provide them an express right to judicial review either. *See Ark. Dairy*, 573 F.3d at 822. While our Circuit Court rejected this argument, stating that "this approach reads *Block* too broadly," it

expressly contemplate participation by even the *recipients* of Section 1861 production orders, let alone third parties. Rather, as originally enacted, FISA was characterized by a secret, ex parte process in which only the government participated. Period. *See* 50 U.S.C. § 1805(a), (e)(4); *In re Sealed Case*, 310 F.3d 717, 719 (FISA Ct. Rev. 2002) ("[T]he government is the only party to FISA proceedings . . . ."). In passing the USA PATRIOT Improvement and Reauthorization Act, however, Congress provided an avenue for recipients of Section 1861 production orders to participate in litigation before the FISC and thus play a role in the statutory scheme. *See* USA PATRIOT Improvement and Reauthorization Act § 106(f); Kris & Wilson, § 19:7.[28] As such, it would not be prudent to treat Congressional silence regarding third parties as an intent to provide

---

reasoned that "the Supreme Court [in *Block*] did not concentrate simply on the presence or absence of an explicit right of appeal in the AMAA, but instead noted that in the 'complex scheme' of the AMAA, there was no provision for consumer participation of any kind." *Id.* In that particular case, our Circuit Court found that the AMAA did, in fact, contemplate the participation of milk producers in the regulatory process, and the court relied on this factor, in part, in holding that producers could bring suit under the APA. *Id.* at 822-27. Here, by contrast, the FISA statutory scheme does not contemplate any participation by third parties in the process of regulating governmental surveillance for foreign intelligence purposes, nor does Section 1861 contemplate the participation of third parties in adjudicating the legality of production orders. Indeed, only in the last decade has the FISA statutory scheme permitted participation by even recipients of production orders.

[28] The USA PATRIOT Improvement and Reauthorization Act also added a provision allowing recipients of National Security Letters ("NSLs") to seek judicial review of those letters. *See* USA PATRIOT Improvement and Reauthorization Act § 115. In contrast to the provision of a right of judicial review to recipients of Section 1861 production orders *before the FISC*, the act provided that the recipient of an NSL (under any of the five NSL statutes) "may, in the United States district court for the district in which that person or entity does business or resides, petition for an order modifying or setting aside the request." 18 U.S.C. § 3511.

broader judicial review than that specifically set forth in the statute.[29] Judicial alchemy of that sort is particularly inappropriate on matters affecting national security.

To be sure, FISA and Section 1861 *do* implicate the interests of cell phone subscribers when their service providers are producing metadata about their phone communications to the Government, as I will discuss below in the context of plaintiffs' constitutional claims. But the statutory preclusion inquiry "does not only turn on whether the interests of a particular class . . . are implicated." *Block*, 467 U.S. at 347. "Rather, the preclusion issue turns ultimately on whether Congress intended for that class to be relied upon to challenge agency disregard of the law." *Id.* Here, the detailed procedures set out in the statute for judicial review of Section 1861 production orders, at the behest of recipients of those orders, indicate that, for better or worse, Congress did not intend for

[29] Indeed, it would be curious to reach the opposite conclusion—that even though the statute expressly permits only recipients to challenge Section 1861 production orders in a specific forum (after Congress rejected an amendment that proposed to allow them to bring their challenges in federal district court at the same time it decided to allow recipients of NSLs to do exactly that), and even though Congress considered but declined to extend that right of judicial review to third parties, *see* Govt.'s Suppl. Br. at 3, these plaintiffs can nonetheless, in effect, challenge those orders in district court by bringing a claim under the APA challenging government agency conduct. In *Block*, when finding that the AMAA statute precluded claims by milk consumers, the Supreme Court noted that permitting consumers to seek judicial review of milk orders directly when the statute required milk handlers to first exhaust administrative remedies, "would severely disrupt this complex and delicate administrative scheme." *Block*, 467 U.S. at 348; *cf. Sackett v. EPA*, 132 S. Ct. 1367, 1374 (2012) ("Where a statute provides that particular agency action is reviewable at the instance of one party, who must first exhaust administrative remedies, the inference that it is not reviewable at the instance of other parties, who are not *subject* to the administrative process, is strong."). Permitting third parties to come into federal district court to challenge the legality of Section 1861 production orders, or government agency action conducted pursuant thereto, under the banner of an APA claim would likewise frustrate the statutory scheme here, where Congress in FISA has set out a specific process for judicial review of those orders by the FISC.

third parties, such as plaintiff phone subscribers here, to challenge the Government's compliance with the statute.[30]

II. Constitutional Claims

A. Jurisdiction

Finding that I lack jurisdiction to review plaintiffs' APA claim does not, however, end the Court's jurisdictional inquiry. Plaintiffs have raised several constitutional challenges to the Government's conduct at issue here. And while the Government has

[30] Finally, against this backdrop of FISA's structure, purpose, and history, I find the Government's second preclusion argument—that 18 U.S.C. § 2712 also shows Congress's intent to preclude an APA statutory claim under Section 1861, Govt.'s Opp'n at 30—more persuasive than it otherwise appears when reading that statute alone. Section 2712, which Congress added to the Stored Communications Act in 2001, provides that "[a]ny person who is aggrieved by any willful violation of [the Stored Communications Act] or of [the Wiretap Act] or of sections 106(a) [50 U.S.C. § 1806(a)], 305(a) [50 U.S.C. § 1825(a)], or 405(a) [50 U.S.C. § 1845(a)] of the Foreign Intelligence Surveillance Act . . . may commence an action in United States District Court against the United States to recover money damages." The Government argues that because this statute creates a *money damages* action against the United States for violations of three specific provisions of FISA, it impliedly precludes an action for *injunctive relief* regarding *any* provision of FISA, such as Section 1861. *See* Govt.'s Opp'n at 30-31; Govt.'s Suppl. Br. at 3-4. According to the Government, "Section 2712 thus deals with claims for misuses of information obtained under FISA in great detail, including the intended remedy," and therefore plaintiffs here cannot rely on Section 1861 "to bring a claim for violation of FISA's terms that Congress did not provide for under 18 U.S.C. § 2712." Govt.'s Opp'n at 31. Indeed, Judge White in the Northern District of California came to this same conclusion, holding that Section 2712, "by allowing suits against the United States only for damages based on three provisions of [FISA], impliedly bans suits against the United States that seek injunctive relief under any provision of FISA." *Jewel v. Nat'l Sec. Agency*, --- F. Supp. 2d ---, 2013 WL 3829405, at *12 (N.D. Cal. July 23, 2013). Of course, Section 2712 also expressly provides that "[a]ny action against the United States under this subsection shall be the exclusive remedy against the United States for any claims *within the purview of this section*," 18 U.S.C. § 2712(d) (emphasis added), and therefore it might be argued that Section 2712's provision of a remedy should not be read more broadly to have any preclusive impact on violations of other provisions of FISA, such as Section 1861, not "within the purview" of that section. But when read in conjunction with FISA overall, and in light of the secret nature of FISA proceedings designed to advance intelligence-gathering for national security purposes, I agree with the Government that Section 2712's provision of a certain remedy, money damages, for violations of only certain provisions of FISA should be read to further show Congress's intent to preclude judicial review of APA claims for injunctive relief by third parties regarding any provision of FISA, including Section 1861.

conceded this Court's authority to review these constitutional claims, Govt.'s Suppl. Br. at 4, I must nonetheless independently evaluate my jurisdictional authority, *see Henderson ex rel. Henderson v. Shinseki*, 131 S. Ct. 1197, 1202 (2011) ("[F]ederal courts have an independent obligation to ensure that they do not exceed the scope of their jurisdiction, and therefore they must raise and decide jurisdictional questions that the parties either overlook or elect not to press.").

Because Article III courts were created, in part, to deal with allegations of constitutional violations, U.S. CONST. art. III, § 2, the jurisdictional inquiry here turns, in the final analysis, on whether Congress intended to preclude judicial review of constitutional claims related to FISC orders by any non-FISC courts. Not surprisingly, the Supreme Court has addressed Congressional efforts to limit constitutional review by Article III courts. In *Webster v. Doe*, 486 U.S. 592 (1988), the Court stated emphatically that "where Congress intends to preclude judicial review of constitutional claims its intent to do so must be clear." *Id.* at 603. Such a "heightened showing" is required "in part to avoid the 'serious constitutional question' that would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim." *Id.* (holding that although a former CIA employee who alleged that he was fired because he was a homosexual, in violation of the APA and the Constitution, could not obtain judicial review under the APA because such decisions were committed to the agency's discretion by law, 5 U.S.C. § 701(a)(2), under a provision of the National Security Act of 1947, a court could nonetheless review the plaintiff's constitutional claims based on the same allegation).

As discussed in Part I above, FISA does not include an express right of judicial review for third party legal challenges to Section 1861 orders—whether constitutional or otherwise, whether in the FISC or elsewhere. But neither does FISA contain any language *expressly barring* all judicial review of third party claims regarding Section 1861 orders—a necessary condition to even raise the question of whether FISA's statutory scheme of judicial review provides the exclusive means of review for constitutional claims relating to Section 1861 production orders. *See Elgin v. Dep't of the Treasury*, 132 S. Ct. 2126, 2132 (2012) ("[A] necessary predicate to the application of *Webster*'s heightened standard [is] a statute that purports to 'deny any judicial forum for a colorable constitutional claim.'"); *see also McBryde v. Comm. to Review Circuit Council Conduct & Disability Orders of the Judicial Conference of U.S.*, 264 F.3d 52, 59 (D.C. Cir. 2001) (the D.C. Circuit "find[s] preclusion of review for both as applied and facial constitutional challenges only if the evidence of congressional intent to preclude is 'clear and convincing' . . . . [and] we have not regarded broad and seemingly comprehensive statutory language as supplying the necessary clarity to bar as applied constitutional claims"); *Ungar v. Smith*, 667 F.2d 188, 193-96 (D.C. Cir. 1981) (holding that statutory language in 22 U.S.C. § 1631o(c) stating administrative determinations "shall be final and shall not be subject to review by any court" did *not* bar courts from hearing constitutional claims relating to the statute, absent a clear expression of Congress's intent to bar such claims in the statute's legislative history). Because FISA contains no "broad and seemingly comprehensive statutory language" expressly barring judicial review of *any* claims under Section 1861, let alone any language directed at

constitutional claims in particular, Congress has *not* demonstrated an intent to preclude constitutional claims sufficient to even trigger the *Webster* heightened standard in the first place, let alone "clear" enough to meet it.

This, of course, makes good sense. The presumption that judicial review of constitutional claims is available in federal district courts is a strong one, *Webster*, 486 U.S. at 603, and if the *Webster* heightened standard is to mean anything, it is that Congress's intent to preclude review of constitutional claims must be much clearer than that sufficient to show *implied* preclusion of *statutory* claims. Where, as here, core individual constitutional rights are implicated by Government action, Congress should not be able to cut off a citizen's right to judicial review of that Government action simply because it intended for the conduct to remain secret by operation of the design of its statutory scheme. While Congress has great latitude to create statutory schemes like FISA, it may not hang a cloak of secrecy over the Constitution.

B. Preliminary Injunction

When ruling on a motion for preliminary injunction, a court must consider "whether (1) the plaintiff has a substantial likelihood of success on the merits; (2) the plaintiff would suffer irreparable injury were an injunction not granted; (3) an injunction would substantially injure other interested parties; and (4) the grant of an injunction would further the public interest." *Sottera, Inc. v. Food & Drug Admin.*, 627 F.3d 891,

893 (D.C. Cir. 2010) (internal quotation marks omitted).[31] I will address each of these factors in turn.

1. Plaintiffs Have Shown a Substantial Likelihood of Success on the Merits.

In addressing plaintiffs' likelihood of success on the merits of their constitutional claims, I will focus on their Fourth Amendment arguments, which I find to be the most likely to succeed.[32] First, however, I must address plaintiffs' standing to challenge the various aspects of the Bulk Telephony Metadata Program. *See Jack's Canoes & Kayaks, LLC v. Nat'l Park Serv.*, 933 F. Supp. 2d 58, 76 (D.D.C. 2013) ("The first component of the likelihood of success on the merits prong usually examines whether the plaintiffs have standing in a given case." (internal quotation marks omitted)).

a. Plaintiffs Have Standing to Challenge Bulk Telephony Metadata Collection and Analysis.

"To establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (internal

---

[31] Our Circuit has traditionally applied a "sliding scale" approach to these four factors. *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1291 (D.C. Cir. 2009). In other words, "a strong showing on one factor could make up for a weaker showing on another." *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011). Following the Supreme Court's decision in *Winter v. NRDC, Inc.*, 555 U.S. 7 (2008), however, our Circuit "has suggested, without deciding, that *Winter* should be read to abandon the sliding-scale analysis in favor of a 'more demanding burden' requiring Plaintiffs to independently demonstrate both a likelihood of success on the merits and irreparable harm." *Smith v. Henderson*, --- F. Supp. 2d ---, 2013 WL 2099804, at *4 (D.D.C. May 15, 2013) (citing *Sherley*, 644 F.3d at 392). Regardless of how *Winter* is read, the Court's analysis here is unaffected because I conclude that plaintiffs have made a sufficient showing of both a likelihood of success on the merits and irreparable harm.

[32] *See supra* note 7.

quotation marks omitted). In *Clapper*, the Supreme Court held that plaintiffs lacked standing to challenge NSA surveillance under FISA because their "highly speculative fear" that they would be targeted by surveillance relied on a "speculative chain of possibilities" insufficient to demonstrate a "certainly impending" injury. *Id.* at 1147-50. Moreover, the *Clapper* plaintiffs' "self-inflicted injuries" (i.e., the costs and burdens of avoiding the feared surveillance) could not be traced to any provable government activity. *Id.* at 1150-53.[33] That is not the case here.

The NSA's Bulk Telephony Metadata Program involves two potential searches: (1) the bulk collection of metadata and (2) the analysis of that data through the NSA's querying process. For the following reasons, I have concluded that the plaintiffs have standing to challenge both. First, as to the collection, the Supreme Court decided *Clapper* just months *before* the June 2013 news reports revealed the existence and scope of certain NSA surveillance activities. Thus, whereas the plaintiffs in *Clapper* could only speculate as to whether they would be surveilled at all, plaintiffs in this case can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected

[33] I note in passing one significant difference between the metadata collection at issue in this case and the electronic surveillance at issue in *Clapper*. As the Court noted in *Clapper*, "if the Government intends to use or disclose information obtained or derived from a [50 U.S.C.] § 1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition." 133 S. Ct. at 1154 (citing 50 U.S.C. §§ 1806(c), 1806(e), 1881e(a)). Sections 1806(c) and (e) and 1881e(a), however, apply only to "information obtained or derived from an electronic surveillance" authorized by specific statutes; they do *not* apply to business records collected under Section 1861. Nor does it appear that any other statute requires the Government to notify a criminal defendant if it intends to use evidence derived from an analysis of the bulk telephony metadata collection.

barring judicial or legislative intervention. *Compare id.* at 1148 ("[R]espondents have no actual knowledge of the Government's § 1881a targeting practices."), *with* Pls.' Mem. at 1, 2 n.2, 7-8 (citing FISC orders and statements from Director of National Intelligence); Suppl. Klayman Aff. ¶ 3 (attesting to status as Verizon customer); Strange Aff. ¶ 2 (same). In addition, the Government has declassified and authenticated an April 25, 2013 FISC Order signed by Judge Vinson, which confirms that the NSA has indeed collected telephony metadata from Verizon. *See* Apr. 25, 2013 Secondary Order.

Straining mightily to find a reason that plaintiffs nonetheless lack standing to challenge the metadata collection, the Government argues that Judge Vinson's order names only Verizon Business Network Services ("VBNS") as the recipient of the order, whereas plaintiffs claim to be Verizon Wireless subscribers. *See* Govt.'s Opp'n at 21 & n.9. The Government obviously wants me to infer that the NSA may not have collected records from Verizon Wireless (or perhaps any other non-VBNS entity, such as AT&T and Sprint). Curiously, the Government makes this argument at the same time it is describing in its pleadings a bulk metadata collection program that can function *only* because it "creates an historical repository that permits retrospective analysis of terrorist-related communications *across multiple telecommunications networks*, and that can be immediately accessed as new terrorist-associated telephone identifiers come to light." Govt.'s Opp'n at 12 (emphasis added); *see also id.* at 65 (court orders to segregate and destroy individual litigants' records "could ultimately have a degrading effect on the utility of the program"); Shea Decl. ¶ 65 (removing plaintiffs' phone numbers "could undermine the results of any authorized query of a phone number that based on RAS is

associated with one of the identified foreign terrorist organizations by eliminating, or cutting off potential call chains").

Put simply, the Government wants it both ways. Virtually all of the Government's briefs and arguments to this Court explain how the Government has acted in good faith to create a *comprehensive* metadata database that serves as a potentially valuable tool in combating terrorism—in which case, the NSA *must* have collected metadata from Verizon Wireless, the single largest wireless carrier in the United States, as well as AT&T and Sprint, the second and third-largest carriers. *See Grading the top U.S. carriers in the third quarter of 2013*, FIERCEWIRELESS.COM (Nov. 18, 2013);[34] Marguerite Reardon, *Competitive wireless carriers take on AT&T and Verizon*, CNET.COM (Sept. 10, 2012).[35] Yet in one footnote, the Government asks me to find that plaintiffs lack standing based on the theoretical possibility that the NSA has collected a universe of metadata so incomplete that the program could not possibly serve its putative function.[36] Candor of this type defies common sense and does not exactly inspire confidence!

Likewise, I find that plaintiffs also have standing to challenge the NSA's querying procedures, though not for the reasons they pressed at the preliminary injunction hearing.

[34] http://www.fiercewireless.com/special-reports/grading-top-us-carriers-third-quarter-2013.

[35] http://news.cnet.com/8301-1035_3-57505803-94/competitive-wireless-carriers-take-on-at-t-and-verizon/.

[36] To draw an analogy, if the NSA's program operates the way the Government suggests it does, then omitting Verizon Wireless, AT&T, and Sprint from the collection would be like omitting John, Paul, and George from a historical analysis of the Beatles. A Ringo-only database doesn't make any sense, and I cannot believe the Government would create, maintain, and so ardently defend such a system.

At oral argument, I specifically asked Mr. Klayman whether plaintiffs had any "basis to believe that the NSA has done any queries" involving their phone numbers. Transcript of Nov. 18, 2013 Preliminary Injunction Hearing at 22, *Klayman I & Klayman II* ("P.I. Hr'g Tr.") [Dkt. # 41]. Mr. Klayman responded: "I think they are messing with me." *Id.* He then went on to explain that he and his clients had received inexplicable text messages and emails, not to mention a disk containing a spyware program. *Id.*; *see also* Strange Aff. ¶¶ 12-17. Unfortunately for plaintiffs, none of these unusual occurrences or instances of being "messed with" have anything to do with the question of whether the NSA has ever queried or analyzed their telephony metadata, so they do not confer standing on plaintiffs.

The Government, however, describes the advantages of bulk collection in such a way as to convince me that plaintiffs' metadata—indeed *everyone's* metadata—is analyzed, manually or automatically,[37] whenever the Government runs a query using as the "seed" a phone number or identifier associated with a phone for which the NSA has not collected metadata (e.g., phones operating through foreign phone companies). According to the declaration submitted by NSA Director of Signals Intelligence Directorate ("SID") Teresa H. Shea, the data collected as part of the Bulk Telephony Metadata Program—had it been in place at that time—would have allowed the NSA to determine that a September 11 hijacker living in the United States had contacted a known al Qaeda safe house in Yemen. Shea Decl. ¶ 11. Presumably, the NSA is not collecting

[37] *See* Oct. 11, 2013 Primary order at 11 ("Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below."); *see also supra* note 22.

metadata from whatever Yemeni telephone company was servicing that safehouse, which means that the metadata program remedies the investigative problem in Director Shea's example *only if* the metadata can be queried to determine which callers in the United States had ever contacted or been contacted by the target Yemeni safehouse number. *See also* Shea Decl. ¶ 44 (the metadata collection allows NSA analysts to, among other things, "detect foreign identifiers associated with a foreign terrorist organization calling into the U.S. and discover which domestic identifiers are in contact with the foreign identifiers."). When the NSA runs such a query, its system must necessarily analyze metadata for *every* phone number in the database by comparing the foreign target number against *all* of the stored call records to determine which U.S. phones, if any, have interacted with the target number.[38] Moreover, unlike a DNA or fingerprint database—which contains only a single "snapshot" record of each person therein—the NSA's database is updated every single day with new information about each phone number. *Compare Johnson v. Quander*, 440 F.3d 489, 498-99 (D.C. Cir. 2006), *with* Govt.'s Opp'n at 8-9. Because the Government can use daily metadata collection to engage in

[38] The difference between querying a phone number belonging to a domestic Verizon subscriber (for which metadata has been collected) and querying a foreign number (for which metadata has not been collected) might be analogized as follows. A query that begins with a domestic U.S. phone number is like entering a library and looking to find all of the sources that are cited in *Battle Cry of Freedom* by James M. McPherson (Oxford University Press 1988). You find that specific book, open it, and there they are. "Hop one" is complete. Then, you want to find all the sources cited within each of those sources ("hop two"), and so on. At the end of a very long day, you have looked only at books, articles, etc. that were linked to *Battle Cry of Freedom*.

Querying a foreign phone number is like entering a library and trying to find every book that cites *Battle Cry of Freedom* as a source. It might be referenced in a thousand books. It might be in just ten. It could be in zero. The only way to know is to check every book. At the end of a very long month, you are left with the "hop one" results (those books that cite *Battle Cry of Freedom*), but to get there, you had to open every book in the library.

"repetitive, surreptitious surveillance of a citizen's private goings on," the NSA database "implicates the Fourth Amendment each time a government official monitors it."[39] *Johnson*, 440 F.3d at 498-99 (distinguishing DNA profile in a law enforcement database—which is not searched each time database is accessed—from a "constantly updat[ing]" video feed, and warning that "future technological advances in DNA testing . . . may empower the government to conduct wide-ranging 'DNA dragnets' that raise justifiable citations to George Orwell"). And the NSA can access its database whenever it wants, repeatedly querying any seed approved in the last 180 days (for terms believed to be used by U.S. persons) or year (for all other terms). *See* Oct. 11, 2013 Primary Order at 10.[40]

---

[39] It is irrelevant for Fourth Amendment purposes that the NSA might sometimes use automated analytical software. *Cf. Smith*, 442 U.S. at 744-45 ("We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.").

[40] The Government contends that "the mere collection of Plaintiffs' telephony metadata . . . without review of the data pursuant to a query" cannot be considered a search "because the Government's acquisition of an item without examining its contents 'does not compromise the interest in preserving the privacy of its contents.'" Govt.'s Opp'n at 49 n.33 (quoting *Horton v. California*, 496 U.S. 128, 141 n.11 (1990); citing *United States v. Van Leeuwen*, 397 U.S. 249, 252-53 (1970)). The cases on which the Government relies are inapposite. *Horton* involved the seizure of tangible items under the plain view doctrine. 496 U.S. at 141-42. The Government quotes dicta about whether the seizure of a physical container constitutes a search of the container's contents. *Id.* at 141 n.11. Likewise, the Court in *Van Leeuwen* addressed whether the detention of a package constituted an unreasonable seizure. 397 U.S. at 252-53.

In the case of the bulk telephony metadata collection, there is no analogous "container" that remains sealed; rather, all of the metadata is handled by the Government, *at least* to the degree needed to integrate the metadata into the NSA's database. *See* Shea Decl. ¶¶ 17, 60 (government may access metadata for purpose of "rendering [it] useable to query" because "each [telecom] provider may not maintain records in a format that is subject to a standardized query"). Thus, unlike the contents of the container described in *Horton*, telephony metadata is not kept in an unmolested, opaque package that obscures it from the Government's view.

Accordingly, plaintiffs meet the standing requirements set forth in *Clapper*, as they can demonstrate that the NSA has collected and analyzed their telephony metadata and will continue to operate the program consistent with FISC opinions and orders. Whether doing so violates plaintiffs' Fourth Amendment rights is, of course, a separate question and the subject of the next section, which addresses the merits of their claims. *See United States v. Lawson*, 410 F.3d 735, 740 n.4 (D.C. Cir. 2005) ("[A]lthough courts sometimes refer to the reasonable expectation of privacy issue as 'standing' to contest a search, the question 'is more properly placed within the purview of substantive Fourth Amendment law than within that of standing.'" (quoting *Minnesota v. Carter*, 525 U.S. 83, 88 (1998)).

b. Plaintiffs Are Likely to Succeed on the Merits of Their Fourth Amendment Claim.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend IV. That right "shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.* A Fourth Amendment "search" occurs either when "the Government obtains information by physically intruding on a constitutionally protected area," *United States v. Jones*, 132 S. Ct. 945, 950 n.3 (2012), or when "the government violates a subjective expectation of privacy that society recognizes as reasonable," *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing

Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). This case obviously does not involve a physical intrusion, and plaintiffs do not claim otherwise.[41]

The threshold issue that I must address, then, is whether plaintiffs have a reasonable expectation of privacy that is violated when the Government indiscriminately collects their telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets. If they do—and a Fourth Amendment search has thus occurred—then the next step of the analysis will be to determine whether such a search is "reasonable." *See id.* at 31 (whether a search has occurred is an "antecedent question" to whether a search was reasonable).[42]

i. The Collection and Analysis of Telephony Metadata Constitutes a Search.

The analysis of this threshold issue of the expectation of privacy must start with the Supreme Court's landmark opinion in *Smith v. Maryland*, 442 U.S. 735 (1979), which the FISC has said "squarely control[s]" when it comes to "[t]he production of telephone service provider metadata." Am. Mem. Op., *In re Application of the [FBI] for an Order*

[41] "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Plaintiffs have not offered any theory as to how they would have a possessory interest in their phone data held by Verizon, and I am aware of none.

[42] While it is true "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear," *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010), phone call and text messaging technology is not "emerging," nor is "its role in society" unclear. I therefore believe that it is appropriate and necessary to elaborate on the Fourth Amendment implications of the NSA's metadata collection program.

Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109 at 6-9 (FISC Aug. 29, 2013) (attached as Ex. A to Gilligan Decl.) [Dkt. # 25-2]. In *Smith*, police were investigating a robbery victim's reports that she had received threatening and obscene phone calls from someone claiming to be the robber. *Id.* at 737. Without obtaining a warrant or court order, police installed a pen register, which revealed that a telephone in Smith's home had been used to call the victim on one occasion.[43] *Id.* The Supreme Court held that Smith had no reasonable expectation of privacy in the numbers dialed from his phone because he voluntarily transmitted them to his phone company, and because it is generally known that phone companies keep such information in their business records. *Id.* at 742-44. The main thrust of the Government's argument here is that under *Smith*, no one has an expectation of privacy, let alone a reasonable one, in the telephony metadata that telecom companies hold as business records; therefore, the Bulk Telephony Metadata Program is not a search. Govt.'s Opp'n at 45-50. I disagree.

The question before me is *not* the same question that the Supreme Court confronted in *Smith*. To say the least, "whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment," *id.* at 736—under the circumstances addressed and contemplated in that case—is a far cry from the issue in this case.

[43] A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted" (i.e., it records limited data on outgoing calls). 18 U.S.C. § 3127(3).

Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.

In *United States v. Jones*, 132 S. Ct. 945 (2012), five justices found that law enforcement's use of a GPS device to track a vehicle's movements for nearly a month violated Jones's reasonable expectation of privacy. *See id.* at 955-56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). Significantly, the justices did so *without* questioning the validity of the Court's earlier decision in *United States v. Knotts*, 460 U.S. 276 (1983), that use of a tracking beeper does not constitute a search because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[44] *Id.* at 281. Instead, they emphasized the many significant ways in which the short-range, short-term tracking device used in *Knotts* differed from the constant month-long surveillance achieved with the GPS device attached to Jones's car. *See Jones*, 132 S. Ct. at 956 n.* (Sotomayor, J., concurring) (*Knotts* "does not foreclose the conclusion that GPS monitoring, in the

[44] In *Jones*, the Government relied heavily on *Knotts* (and *Smith*) as support for the argument that Jones had no expectation of privacy in his movements on the roads because he voluntarily disclosed them to the public. *See generally* Brief for Petitioner, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 3561881; Reply Brief for Petitioner, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 5094951. Five justices found that argument unconvincing.

absence of a physical intrusion, is a Fourth Amendment search"); *id.* at 964 (Alito, J., concurring) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." (citation omitted)); *see also United States v. Maynard*, 615 F.3d 544, 557 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945 ("*Knotts* held only that '[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,' not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it." (citation omitted; quoting *Knotts*, 460 U.S. at 281)).[45]

Just as the Court in *Knotts* did not address the kind of surveillance used to track Jones, the Court in *Smith* was not confronted with the NSA's Bulk Telephony Metadata Program.[46] Nor could the Court in 1979 have ever imagined how the citizens of 2013

---

[45] Lower courts, too, have recognized that the Supreme Court's Fourth Amendment decisions cannot be read too broadly. *See, e.g.*, *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987) ("It does not follow that [*California v. Ciraolo*, 476 U.S. 207 (1986), which held that police did not violate a reasonable expectation of privacy when they engaged in a warrantless aerial observation of marijuana plants growing on curtilage of a home using only the naked eye from a height of 1,000 feet,] authorizes any type of surveillance whatever just because one type of minimally-intrusive aerial observation is possible.").

[46] True, the Court in *Knotts* explicitly "reserved the question whether 'different constitutional principles may be applicable' to 'dragnet-type law enforcement practices' of the type that GPS tracking made possible" in *Jones*. *Jones*, 132 S. Ct. at 952 n.6 (quoting *Knotts*, 460 U.S. at 284); *see also id.* at 956, n.* (Sotomayor, J., concurring). That the Court in *Smith* did not explicitly hold open the question of whether an exponentially broader, high-tech, years-long bulk telephony metadata collection program would infringe on reasonable expectations of privacy does not mean that the Court's holding necessarily extends so far as to answer that novel question. The Supreme Court itself has recognized that prior Fourth Amendment precedents and

would interact with their phones. For the many reasons discussed below, I am convinced that the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search. To the contrary, for the following reasons, I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.

First, the pen register in *Smith* was operational for only a matter of days between March 6, 1976 and March 19, 1976, and there is no indication from the Court's opinion that it expected the Government to retain those limited phone records once the case was over. *See* 442 U.S. at 737. In his affidavit, Acting Assistant Director of the FBI Robert J. Holley himself noted that "[p]en-register and trap-and-trace (PR/TT) devices provide no historical contact information, only a record of contacts with the target occurring after the devices have been installed." Holley Decl. ¶ 9. This short-term, forward-looking (as opposed to historical), and highly-limited data collection is what the Supreme Court was assessing in *Smith*. The NSA telephony metadata program, on the other hand, involves the creation and maintenance of a historical database containing *five years'* worth of data. And I might add, there is the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!

---

doctrines do not always control in cases involving unique factual circumstances created by evolving technology. *See, e.g., Kyllo*, 533 U.S. at 34 ("To withdraw protection of this minimum expectation [of privacy in the home] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."). If this isn't such a case, then what is?

Second, the relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies. *Compare Smith*, 442 U.S. at 737 ("[T]he telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home."), *with* Govt.'s Opp'n at 8-9 ("Under this program, . . . certain telecommunications service providers [] produce to the NSA *on a daily basis* electronic copies of call detail records, or telephony metadata . . . . The FISC *first authorized the program in May 2006*, and since then has renewed the program thirty-five times . . . ." (emphases added; citation and internal quotation marks omitted)). The Supreme Court itself has long-recognized a meaningful difference between cases in which a third party collects information and then turns it over to law enforcement, *see, e.g.*, *Smith*, 442 U.S. 735; *United States v. Miller*, 425 U.S. 435 (1976), and cases in which the government and the third party create a formalized policy under which the service provider collects information for law enforcement purposes, *see Ferguson v. Charleston*, 532 U.S. 67 (2001), with the latter raising Fourth Amendment concerns. In *Smith*, the Court considered a one-time, targeted request for data regarding an individual suspect in a criminal investigation, *see Smith*, 442 U.S. at 737, which in no way resembles the daily, all-encompassing, indiscriminate dump of phone metadata that the NSA now receives as part of its Bulk Telephony Metadata Program. It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government.

Cf. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989) ("Plainly there is a vast difference between the public records that might be found after a diligent search of [various third parties' records] and a computerized summary located in a single clearinghouse of information.").[47]

Third, the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979. In *Smith*, the Supreme Court was actually considering whether local police could collect one person's phone records for calls made after the pen register was installed and for the limited purpose of a small-scale investigation of harassing phone calls. *See Smith*, 442 U.S. at 737. The notion that the Government could collect similar data on hundreds of millions of people and retain that data for a five-year period, updating it with new data every day in perpetuity, was at best, in 1979, the stuff of science fiction. By comparison, the Government has at its disposal today the most advanced twenty-first century tools, allowing it to "store such records and efficiently mine them for information years into the future." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). And these technologies are "cheap in comparison to conventional surveillance techniques and, by design, proceed[] surreptitiously," thereby

[47] When an individual makes his property accessible to third parties, he may still retain some expectation of privacy based on his understanding of how third parties typically handle that property. *See Bond v. United States*, 529 U.S. 334, 338-39 (2000) ("[A] bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. But this is exactly what the agent did here. We therefore hold that the agent's physical manipulation of petitioner's bag violated the Fourth Amendment.").

"evad[ing] the ordinary checks that constrain abusive law enforcement practices: limited police . . . resources and community hostility." *Id.*[48]

Finally, *and most importantly*, not only is the Government's ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well. According to the 1979 U.S. Census, in that year, 71,958,000 homes had telephones available, while 6,614,000 did not. U.S. DEP'T OF COMMERCE & U.S. DEP'T OF HOUS. & URBAN DEV., ANNUAL HOUSING SURVEY: 1979, at 4 (1981) (Table A-1: Characteristics of the Housing Inventory: 1979 and 1970). In December 2012, there were a whopping 326,475,248 mobile subscriber connections in the United States, of which approximately 304 million were for phones and twenty-two million were for computers, tablets, and modems.[49] CTIA – The Wireless Ass'n ("CTIA"), *Wireless Industry Survey Results – December 1985 to December 2012*, at 2, 6 (2013) ("CTIA *Survey Results*");[50] *see also* Sixteenth Report, *In re Implementation of Section 6002(b) of Omnibus Budget Reconciliation Act*, WT Dkt. No. 11-186, at 9 (F.C.C. Mar. 21, 2013) ("[A]t the end of 2011 there were 298.3 million subscribers to mobile telephone, or voice, service, up

[48] The unprecedented scope and technological sophistication of the NSA's program distinguish it not only from the *Smith* pen register, but also from metadata collections performed as part of routine criminal investigations. To be clear, this opinion is focusing only on the program before me and not any other law enforcement practices. Like the concurring justices in *Jones*, I cannot "identify with precision the point at which" bulk metadata collection becomes a search, but there is a substantial likelihood that the line was crossed under the circumstances presented in this case. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

[49] The global total is 6.6 billion. ERICSSON, *Mobility Report on the Pulse of Networked Society*, at 4 (Nov. 2013), *available at* http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-november-2013.pdf.

[50] http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf.

nearly 4.6 percent from 285.1 million at the end of 2010."). The number of mobile subscribers in 2013 is more than *3,000 times* greater than the 91,600 subscriber connections in 1984, INDUS. ANALYSIS DIV., FED. COMMC'NS COMM'N, TRENDS IN TELEPHONE SERVICE 8 (1998), and more than *triple* the 97,035,925 subscribers in June 2000, CTI *Survey Results*, *supra*, at 4.[51] It is now safe to assume that the vast majority of people reading this opinion have *at least* one cell phone within arm's reach (in addition to other mobile devices). Joanna Brenner, *Pew Internet: Mobile* (Sept. 18, 2013) (91% of American adults have a cell phone, 95-97% of adults age 18 to 49);[52] CTIA, *Wireless Quick Facts* (last visited Dec. 10, 2013) ("CTIA *Quick Facts*") (wireless penetration—the number of active wireless units divided by total U.S. and territorial population—was 102.2% as of December 2012).[53] In fact, some undoubtedly will be reading this opinion *on their cell phones*. Maeve Duggan, *Cell Phone Activities 2013* (Sept. 19, 2013) (60% of cell phone owners use them to access internet).[54] Cell phones have also morphed into multi-purpose devices. They are now maps and music players. *Id.* (49% of cell phone owners use their phones to get directions and 48% to listen to music). They are cameras. Keith L. Alexander, *Camera phones become courthouse safety issue*, WASH. POST, Apr. 22, 2013, at B01. They are even lighters that people hold up at rock concerts. Andy

---

[51] Mobile phones are rapidly replacing traditional landlines, with 38.2% of households going "wireless-only" in 2012. CTIA, *Wireless Quick Facts*, http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last visited Dec. 10, 2013); *see also* Jeffrey Sparshott, *More People Say Goodbye to Landlines*, WALL ST. J., Sept. 6, 2013, at A5.

[52] http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx.

[53] http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts.

[54] http://pewinternet.org/Reports/2013/Cell-Activities/Main-Findings.aspx.

Rathbun, *Cool 2 Know – Cell phone virtuosos*, NEWSDAY, Apr. 20, 2005, at B02. They are ubiquitous as well. Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago, *none* of those phones would have been there.[55] Thirty-four years ago, city streets were lined with pay phones. Thirty-four years ago, when people wanted to send "text messages," they wrote letters and attached postage stamps.[56]

Admittedly, what metadata *is* has not changed over time. As in *Smith*, the *types* of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like.[57] But the ubiquity of phones has dramatically altered the *quantity* of

---

[55] *Mobile Telephone*, BRITANNICA.COM, http://www.britannica.com/EBchecked/topic/1482373/mobile-telephone?anchor=ref1079017 (last visited Dec. 13, 2013) ("[A] Japanese system was the first cellular system to be deployed, in 1979."); Tom Farley, *Mobile telephone history*, TELEKTRONIKK, March/April 2005, at 28 ("An 88 cell system in the challenging cityscape of Tokyo began in December, 1979 . . . . The first North American commercial system began in August, 1981 in Mexico City.").

[56] It is not clear from the pleadings whether "telephony metadata" and "comprehensive communications routing information" includes data relating to text messages. *See supra* note 16. If it does, then in 2012, the Government collected an additional *six billion* communications *each day* (69,635 *each second*). *See* Infographic – *Americans sent and received more than 69,000 texts every second in 2012*, CTIA.org (Nov. 25, 2013), http://www.ctia.org/resource-library/facts-and-infographics/archive/americans-texts-2012-infographic.

[57] There are, however, a few noteworthy distinctions between the data at issue in *Smith* and the metadata that exists nowadays. For instance, the pen register in *Smith* did not tell the government whether calls were completed or the duration of any calls, *see Smith*, 442 U.S. at 741, whereas that information is captured in the NSA's metadata collection.

A much more significant difference is that telephony metadata can reveal the user's location, *see generally New Jersey v. Earls*, 70 A.3d 630, 637-38 (N.J. 2013), which in 1979 would have been entirely unnecessary given that landline phones are tethered to buildings. The most recent FISC order explicitly "does not authorize the production of cell site location information," Oct. 11, 2013 Primary order at 3 n.1, and the Government has publicly disavowed such collection, *see* Transcript of June 25, 2013 Newseum Special Program: NSA Surveillance Leaks: Facts and Fiction, Remarks of Robert Litt, Gen. Counsel, Office of Dir. of Nat'l Intelligence, *available at* http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-

information that is now available and, *more importantly*, what that information can tell the Government about people's lives. *See Quon*, 130 S. Ct. at 2630 ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. . . . [And] the ubiquity of those devices has made them generally affordable . . . ."); *cf. Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (discussing the "substantial quantum of intimate information about any person" captured by GPS tracking). Put simply, people in 2013 have an entirely different relationship with phones than they did thirty-four years ago. As a

---

and-fiction ("I want to make perfectly clear we do not collect cellphone location information under this program, either GPS information or cell site tower information.").

That said, not all FISC orders have been made public, and I have no idea how location data has been handled in the past. Plaintiffs *do* allege that location data has been collected, *see* Second Am. Compl. ¶ 28; Pls.' Mem. at 10-11, and the Government's brief does not refute that allegation (though one of its declarations does, *see* Shea Decl. ¶ 15). *See also supra* note 17. Moreover, the most recent FISC order states, and defendants concede, that "'telephony metadata' includes . . . trunk identifier[s]," Oct. 11, 2013 Primary order at 3 n.1; Govt.'s Opp'n at 9, which apparently "can reveal where [each] call enter[s] the trunk system" and can be used to "locate a phone within approximately a square kilometer," Patrick Di Justo, *What the N.S.A. Wants to Know About Your Calls*, NEW YORKER (June 7, 2013), http://www.newyorker.com/online/blogs/elements/2013/06/what-the-nsa-wants-to-know-about-your-phone-calls.html. And "if [the metadata] includes a request for every trunk identifier used throughout the interaction," that "could allow a phone's movements to be tracked." *Id.* Recent news reports, though not confirmed by the Government, cause me to wonder whether the Government's briefs are entirely forthcoming about the full scope of the Bulk Telephony Metadata Program. *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA maps targets by their phones*, WASH. POST, Dec. 5, 2013, at A01.

The collection of location data would, of course, raise its own Fourth Amendment concerns, *see, e.g.*, *In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information."), but my decision on this preliminary injunction does *not* turn on whether the NSA has in fact collected that data as part of the bulk telephony metadata program.

result, people make calls and send text messages now that they would not (really, *could not*) have made or sent back when *Smith* was decided—for example, every phone call today between two people trying to locate one another in a public place. *See* CTIA *Quick Facts, supra* (2.3 *trillion* voice minutes used in 2012, up from 62.9 billion in 1997). This rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person's phone "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring), that could not have been gleaned from a data collection in 1979. *See also* Decl. of Prof. Edward W. Felten ("Felten Decl.") [Dkt. # 22-1], at ¶¶ 38-58. Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life. *See Maynard*, 615 F.3d at 562-63.[58] Whereas some may assume that these cultural changes will force people to "reconcile themselves" to an "inevitable" "diminution of privacy that new technology entails," *Jones*, 132 S. Ct. at 962 (Alito, J., concurring), I think it is more

[58] The Government maintains that the metadata the NSA collects does not contain personal identifying information associated with each phone number, and in order to get that information the FBI must issue a national security letter ("NSL") to the phone company. Govt.'s Opp'n at 48-49; P.I. Hr'g Tr. at 44-45. Of course, NSLs do not require *any* judicial oversight, *see* 18 U.S.C. § 2709; 12 U.S.C. § 3414, 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 50 U.S.C. § 3162, meaning they are hardly a check on potential abuses of the metadata collection. There is also nothing stopping the Government from skipping the NSL step altogether and using public databases or any of its other vast resources to match phone numbers with subscribers. *See, e.g.*, James Ball et al., *Covert surveillance: The reaction: 'They are tracking the calling patterns of the entire country'*, GUARDIAN, June 7, 2013, at 5 ("[W]hen cross-checked against other public records, the metadata can reveal someone's name, address, driver's licence, credit history, social security number and more."); Felten Decl. ¶ 19 & n.14; Suppl. Decl. of Prof. Edward W. Felten [Dkt. # 28], at ¶¶ 3-4 ("[I]t would be trivial for the government to obtain a subscriber's name once it has that subscriber's phone number . . . . It is extraordinarily easy to correlate a phone number with its unique owner.").

likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable.[59]

In sum, the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones. Plaintiffs have alleged that they engage in conduct that exhibits a subjective expectation of privacy in the bulk, five-year historical record of their telephony metadata, *see* Pls.' Mem. at 21; Suppl. Klayman Aff. ¶¶ 5, 10, 13; Strange Aff. ¶¶ 11, 19, and I have no reason to question the genuineness of those subjective beliefs.[60] The more difficult question, however, is whether their expectation of privacy is one that

[59] Public opinion polls bear this out. *See, e.g.*, Associated Press, *9/11 Anniversary: Poll finds public doubts growing on federal surveillance, privacy*, HOUS. CHRON., Sept. 11, 2013, at A6 ("Some 56 percent oppose the NSA's collection of telephone records for future investigations even though they do not include actual conversations.").

[60] If plaintiffs *lacked* such a subjective expectation of privacy in all of their cell phone metadata, I would likely find that it is the result of "'condition[ing]' by influences alien to well-recognized Fourth Amendment freedoms." *Smith*, 442 U.S. at 740 n.5. In 1979, the Court announced that numbers dialed on a phone are not private, and since that time, the Government and courts have gradually (but significantly) expanded the scope of what that holding allows. Now, even local police departments are routinely requesting and obtaining massive cell phone "tower dumps," each of which can capture data associated with thousands of innocent Americans' phones. *See* Ellen Nakashima, *'Tower dumps' give police masses of cellphone data*, WASH. POST, Dec. 9, 2013, at A01. Targeted tower dumps may be appropriate under certain circumstances and with appropriate oversight and limitations, *see In re Search of Cellular Tel. Towers*, --- F. Supp. 2d ---, 2013 WL 1932881, at *2 (S.D. Tex. May 8, 2013) (requiring warrant and return of all irrelevant records to telecom provider for 77-tower dump of all data for five-minute period), and fortunately, that question is not before me here. The point is, however, that the experiences of many Americans—especially those who have grown up in the post-*Smith*, post-cell phone, post-PATRIOT Act age—might well be compared to those of the "refugee from a totalitarian country, unaware of this Nation's traditions, [who] erroneously assume[] that police were continuously monitoring" telephony metadata. *Smith*, 442 U.S. at 740 n.5. Accordingly, their "subjective expectations obviously could play no meaningful role in ascertaining . . . the scope of Fourth Amendment protection," and "a normative inquiry would be proper." *Id.*

society is prepared to recognize as objectively reasonable and justifiable. As I said at the outset, the question before me is not whether *Smith* answers the question of whether people can have a reasonable expectation of privacy in telephony metadata under all circumstances. Rather, the question that I will ultimately have to answer when I reach the merits of this case someday is whether people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval. For the many reasons set forth above, it is significantly likely that on that day, I will answer that question in plaintiffs' favor.

ii. There Is a Significant Likelihood Plaintiffs Will Succeed in Showing that the Searches Are Unreasonable.

Having found that a search occurred in this case, I next must "examin[e] the totality of the circumstances to determine whether [the] search is reasonable within the meaning of the Fourth Amendment." *Samson v. California*, 547 U.S. 843, 848 (2006) (internal quotation marks omitted). "'[A]s a general matter, warrantless searches are *per se* unreasonable under the Fourth Amendment.'" *Nat'l Fed'n of Fed. Emps.-IAM v. Vilsack*, 681 F.3d 483, 488-89 (D.C. Cir. 2012) (quoting *Quon*, 130 S. Ct. at 2630); *see also Chandler v. Miller*, 520 U.S. 305, 313 (1997) ("To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing.").

The Supreme Court has recognized only a "'few specifically established and well-delineated exceptions to that general rule,'" *Nat'l Fed'n of Fed. Emps.-IAM*, 681 F.3d at 489 (quoting *Quon*, 130 S. Ct. at 2630), including one that applies when "'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable,'" *id.* (quoting *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)). "Even where the government claims 'special needs,'" as it does in this case, "a warrantless search is generally unreasonable unless based on 'some quantum of individualized suspicion.'" *Id.* (quoting *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 624 (1989)). Still, a suspicionless search may be reasonable "'where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion.'" *Id.* (quoting *Skinner*, 489 U.S. at 624). As such, my task is to "'balance the [plaintiffs'] privacy expectations against the government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.'" *Id.* (quoting *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665-66 (1989)). This is a "'context-specific inquiry'" that involves "'examining closely the competing private and public interests advanced by the parties.'" *Id.* (quoting *Chandler*, 520 U.S. at 314)). The factors I must consider include: (1) "the nature of the privacy interest allegedly compromised" by the search, (2) "the character of the intrusion imposed" by the government, and (3) "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Bd. of Educ. v. Earls*, 536 U.S. 822, 830-34 (2002).

"Special needs" cases, not surprisingly, form something of a patchwork quilt. For example, schools and government employers are permitted under certain circumstances to test students and employees for drugs and alcohol, *see Earls*, 536 U.S. 822; *Vernonia Sch. Dist.*, 515 U.S. 646; *Von Raab*, 489 U.S. 656; *Skinner*, 489 U.S. 602, and officers may search probationers and parolees to ensure compliance with the rules of supervision, *see Griffin v. Wisconsin*, 483 U.S. 868 (1987).[61] The doctrine has also been applied in cases involving efforts to prevent acts of terrorism in crowded transportation centers. *See, e.g.*, *Cassidy v. Chertoff*, 471 F.3d 67 (2d Cir. 2006) (upholding searches of carry-on bags and automobiles that passengers bring on ferries); *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006) (upholding searches of bags in New York City subway system). To my knowledge, however, no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion. In effect, the Government urges me to be the first non-FISC judge to sanction such a dragnet.

For reasons I have already discussed at length, I find that plaintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata covering the last five years, and the NSA's Bulk Telephony Metadata Program

[61] Suspicionless searches and seizures have also been allowed in other contexts not analyzed under the "special needs" framework, including administrative inspections of "closely regulated" businesses, *see New York v. Burger*, 482 U.S. 691 (1987), searches of fire-damaged buildings for the purpose of determining the cause of the fire, *see Michigan v. Tyler*, 436 U.S. 499 (1978), and highway checkpoints set up to catch intoxicated motorists and illegal entrants into the United States, *see Mich. Dep't of State Police v. Sitz*, 496 U.S. 444 (1990); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976).

significantly intrudes on that expectation.[62] Whether the program violates the Fourth Amendment will therefore turn on "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Earls*, 536 U.S. at 834.

The Government asserts that the Bulk Telephony Metadata Program serves the "programmatic purpose" of "identifying unknown terrorist operatives and preventing terrorist attacks." Govt.'s Opp'n at 51—an interest that everyone, including this Court, agrees is "of the highest order of magnitude," *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008); *see also Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." (internal quotation marks omitted)).[63] A closer examination of the record, however, reveals that

[62] These privacy interests are not "mitigated . . . by the statutorily mandated restrictions on access to and dissemination of the metadata that are written into the FISC's orders." Govt.'s Opp'n at 51–52. First, there are no minimization procedures applicable at the collection stage; the Government acknowledges that FISC orders require the recipients to turn over all of their metadata without limit. *See* Oct. 11, 2013 Primary order at 3-4. Further, the most recent order of the FISC states that any trained NSA personnel can access the metadata, with "[t]echnical personnel" authorized to run queries even using non-RAS-approved selection terms for purposes of "perform[ing] those processes needed to make [the metadata] usable for intelligence analysis." *Id.* at 5. The "[r]esults of any intelligence analysis queries," meanwhile, "may be shared, *prior to minimization*, for intelligence analysis purposes among [trained] NSA analysts." *Id.* at 12–13 (emphasis added); *see also* Shea Decl. ¶¶ 30, 32 (minimization procedures "guard against inappropriate or unauthorized *dissemination* of information relating to U.S. persons," and "results of authorized queries of the metadata may be shared, *without minimization*, among trained NSA personnel for analysis purposes" (emphases added)). These procedures in no way mitigate the privacy intrusion that occurs when the NSA collects, queries, and analyzes metadata. And that's even *assuming* the Government complies with all of its procedures—an assumption that is not supported by the NSA's spotty track record to date. *See supra* notes 23-25 and accompanying text.

[63] It bears noting that the Government's interest in stopping and prosecuting terrorism *has not* led courts to abandon familiar doctrines that apply in criminal cases generally. *See United States v. Ressam*, 679 F.3d 1069, 1106 (9th Cir. 2012) (Schroeder, J., dissenting) (collecting cases in

the Government's interest is a bit more nuanced—it is not merely to investigate potential terrorists, but rather, to do so *faster* than other investigative methods might allow. Indeed, the affidavits in support of the Government's brief repeatedly emphasize this interest in speed. For example, according to SID Director Shea, the primary advantage of the bulk metadata collection is that "it enables the Government to *quickly* analyze past connections and chains of communication," and "increases the NSA's ability to *rapidly* detect persons affiliated with the identified foreign terrorist organizations." Shea Decl. ¶ 46 (emphases added); *see also id.* ¶ 59 ("Any other means that might be used to attempt to conduct similar analyses would require *multiple, time-consuming steps* that would frustrate needed *rapid* analysis in emergent situations, and could fail to capture some data available through bulk metadata analysis." (emphases added)). FBI Acting Assistant Director of the Counterterrorism Division Robert J. Holley echoes Director Shea's emphasis on speed: "It is imperative that the United States Government have the capability to *rapidly* identify any terrorist threat inside the United States." Holley Decl. ¶ 4 (emphasis added); *see also id.* ¶¶ 28-29 ("[T]he *agility* of querying the metadata collected by NSA under this program allows for more *immediate* contact chaining, which is significant in *time-sensitive* situations . . . . The *delay* inherent in issuing new national security letters would necessarily mean losing *valuable time*. . . . [A]ggregating the NSA

---

which "courts have treated other issues in terrorism cases in ways that do not differ appreciably from more broadly applicable doctrines"). In fact, the Supreme Court once expressed in dicta that an otherwise impermissible roadblock "would *almost* certainly" be allowed "to thwart an *imminent* terrorist attack." *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000) (emphases added). The Supreme Court has never suggested that all Fourth Amendment protections must defer to any Government action that purportedly serves national security or counterterrorism interests.

telephony metadata from different telecommunications providers enhances and *expedites* the ability to identify chains of communications across multiple providers." (emphases added)).

Yet, turning to the efficacy prong, the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three "recent episodes" cited by the Government that supposedly "illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack" involved any apparent urgency. *See* Holley Decl. ¶¶ 24-26. In the first example, the FBI learned of a terrorist plot still "in its early stages" and investigated that plot before turning to the metadata "to ensure that all potential connections were identified." *Id.* ¶ 24. Assistant Director Holley does not say that the metadata revealed any new information—much less time-sensitive information—that had not already come to light in the investigation up to that point. *Id.* In the second example, it appears that the metadata analysis was used only after the terrorist was arrested "to establish [his] foreign ties and put them in context with his U.S. based planning efforts." *Id.* ¶ 25. And in the third, the metadata analysis "revealed a previously unknown number for [a] co-conspirator . . . and corroborated his connection to [the target of the investigation] as well as to other U.S.-based extremists." *Id.* ¶ 26. Again, there is no indication that these revelations were immediately useful or that they prevented an impending attack. Assistant Director Holley even concedes that bulk metadata analysis only "*sometimes* provides information earlier than the FBI's other investigative methods

and techniques." *Id.* ¶ 23 (emphasis added).[64] Given the limited record before me at this point in the litigation—most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics—I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.[65] *See Chandler*, 520 U.S. at 318-19 ("Notably lacking in respondents' presentation is any indication of a concrete danger demanding departure from the Fourth Amendment's main rule."). Thus, plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment.[66]

---

[64] Such candor is as refreshing as it is rare.

[65] The Government could have requested permission to present additional, potentially classified evidence *in camera*, but it chose not to do so. Although the Government has publicly asserted that the NSA's surveillance programs have prevented fifty-four terrorist attacks, no proof of that has been put before me. *See also* Justin Elliott & Theodoric Meyer, *Claim on 'Attacks Thwarted' by NSA Spreads Despite Lack of Evidence*, PROPUBLICA.ORG (Oct. 23, 2013), http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence ("'We've heard over and over again the assertion that 54 terrorist plots were thwarted' by the [NSA's] programs . . . . 'That's plainly wrong . . . . These weren't all plots and they weren't all thwarted. The American people are getting left with the inaccurate impression of the effectiveness of the NSA programs.'" (quoting Sen. Patrick Leahy)); Ellen Nakashima, *NSA's need to keep database questioned*, WASH. POST, Aug. 9, 2013, at A01 ("[Senator Ron] Wyden noted that [two suspects arrested after an investigation that involved use of the NSA's metadata database] were arrested 'months or years after they were first identified' by mining the phone logs.").

[66] The Government points out that it could obtain plaintiffs' metadata through other means that potentially raise fewer Fourth Amendment concerns. *See* Govt.'s Opp'n at 6 ("The records must be of a type obtainable by either a grand jury subpoena, or an order issued by a U.S. court directing the production of records or tangible things." (citing 50 U.S.C. § 1861(c)(2)(D)); Holley Decl. ¶ 14 ("In theory, the FBI could seek a new set of orders on a daily basis for the records created within the preceding 24 hours."). Even if true, "[t]he fact that equivalent

I realize, of course, that such a holding might appear to conflict with other trial courts, *see, e.g.*, *United States v. Moalin*, Crim. No. 10-4246, 2013 WL 6079518, at *5-8 (S.D. Cal. Nov. 18, 2013) (holding that bulk telephony metadata collection does not violate Fourth Amendment); *United States v. Graham*, 846 F. Supp. 2d 384, 390-405 (D. Md. 2012) (holding that defendants had no reasonable expectation of privacy in historical cell-site location information); *United States v. Gordon*, Crim. No. 09-153-02, 2012 WL 8499876, at *1-2 (D.D.C. Feb. 6, 2012) (same), and with longstanding doctrine that courts have applied in other contexts, *see, e.g.*, *Smith*, 442 U.S. at 741-46 *Miller*, 425 U.S. at 443. Nevertheless, in reaching this decision, I find comfort in the statement in the Supreme Court's recent majority opinion in *Jones* that "[a]t bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" 132 S. Ct. at 950 (2012) (quoting *Kyllo*, 533 U.S. at 34). Indeed, as the Supreme Court noted more than a decade before *Smith*, "[t]he basic purpose of th[e Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against *arbitrary invasions by governmental officials*." *Camara v. Mun. Court*, 387 U.S. 523, 528 (1967) (emphasis added); *see also Quon*, 130 S. Ct. at 2627 ("The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government, without regard to whether the government actor is investigating crime or performing another function." (internal quotation marks omitted)). The Fourth

information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Kyllo*, 533 U.S. at 35 n.2.

Amendment typically requires "a neutral and detached authority be interposed between the police and the public," and it is offended by "general warrants" and laws that allow searches to be conducted "indiscriminately and without regard to their connection with [a] crime under investigation." *Berger v. New York*, 388 U.S. 41, 54, 59 (1967). I cannot imagine a more "indiscriminate" and "arbitrary invasion" than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on "that degree of privacy" that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware "the abridgement of freedom of the people by gradual and silent encroachments by those in power," would be aghast.[67]

2. Plaintiffs Will Suffer Irreparable Harm Absent Injunctive Relief.

"It has long been established that the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury.'" *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009) (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (plurality opinion)). As in this case, the court in *Mills* was confronted with an alleged Fourth Amendment violation: a "Neighborhood Safety Zones" traffic checkpoint for vehicles entering a high-crime neighborhood in Washington, DC. *Id.* at

[67] James Madison, Speech in the Virginia Ratifying Convention on Control of the Military (June 16, 1788), *in* THE HISTORY OF THE VIRGINIA FEDERAL CONVENTION OF 1788, WITH SOME ACCOUNT OF EMINENT VIRGINIANS OF THAT ERA WHO WERE MEMBERS OF THE BODY (Vol. I) 130 (Hugh Blair Grigsby et al. eds., 1890) ("Since the general civilization of mankind, I believe there are more instances of the abridgement of freedom of the people by gradual and silent encroachments by those in power than by violent and sudden usurpations.").

1306. After finding a strong likelihood of success on the merits, our Circuit Court had little to say on the irreparable injury prong, instead relying on the statement at the beginning of this paragraph that a constitutional violation, even of minimal duration, constitutes irreparable injury. Plaintiffs in this case have also shown a strong likelihood of success on the merits of a Fourth Amendment claim. As such, they too have adequately demonstrated irreparable injury.

3. The Public Interest and Potential Injury to Other Interested Parties Also Weigh in Favor of Injunctive Relief.

"'[I]t is always in the public interest to prevent the violation of a party's constitutional rights.'" *Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth.*, 898 F. Supp. 2d 73, 84 (D.D.C. 2012) (quoting *G & V Lounge, Inc. v. Mich. Liquor Control Comm'n*, 23 F.3d 1071, 1079 (6th Cir. 1994)); *see also Hobby Lobby Stores, Inc. v. Sebelius*, 723 F.3d 1114, 1145 (10th Cir. 2013) (same), *cert. granted*, --- S. Ct. ----, 2013 WL 5297798 (2013); *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012) (same); *Nat'l Fed'n of Fed. Emps. v. Carlucci*, 680 F. Supp. 416 (D.D.C. 1988) ("[T]he public interest lies in enjoining unconstitutional searches."). That interest looms large in this case, given the significant privacy interests at stake and the unprecedented scope of the NSA's collection and querying efforts, which likely violate the Fourth Amendment. Thus, the public interest weighs heavily in favor of granting an injunction.

The Government responds that the public's interest in combating terrorism is of paramount importance, *see* Govt.'s Opp'n at 64-65—a proposition that I accept without question. But the Government offers no real explanation as to how granting relief to

these plaintiffs would be detrimental to that interest. Instead, the Government says that it will be burdensome to comply with any order that requires the NSA to remove plaintiffs from its database. *See id.* at 65; Shea Decl. ¶ 65. Of course, the public has no interest in saving the Government from the burdens of complying with the Constitution! Then, the Government frets that such an order "could ultimately have a degrading effect on the utility of the program if an injunction in this case precipitated successful requests for such relief by other litigants." Govt.'s Opp'n at 65 (citing Shea Decl ¶ 65). For reasons already explained, I am not convinced at this point in the litigation that the NSA's database has ever truly served the purpose of rapidly identifying terrorists in time-sensitive investigations, and so I am *certainly* not convinced that the removal of two individuals from the database will "degrade" the program in any meaningful sense.[68] I will leave it to other judges to decide how to handle any future litigation in their courts.

CONCLUSION

This case is yet the latest chapter in the Judiciary's continuing challenge to balance the national security interests of the United States with the individual liberties of our citizens. The Government, in its understandable zeal to protect our homeland, has crafted a counterterrorism program with respect to telephone metadata that strikes the balance based in large part on a thirty-four year old Supreme Court precedent, the

[68] To the extent that removing plaintiffs from the database would create a risk of "eliminating, or cutting off potential call chains," Shea Decl. ¶ 65, the Government concedes that the odds of this happening are miniscule. *See* Govt.'s Opp'n at 2 ("[O]nly a tiny fraction of the collected metadata is ever reviewed . . . ."); Shea Decl. ¶ 23 ("Only the tiny fraction of the telephony metadata records that are responsive to queries authorized under the RAS standard are extracted, reviewed, or disseminated . . . .").

relevance of which has been eclipsed by technological advances and a cell phone-centric lifestyle heretofore inconceivable. In the months ahead, other Article III courts, no doubt, will wrestle to find the proper balance consistent with our constitutional system. But in the meantime, for all the above reasons, I will grant Larry Klayman's and Charles Strange's requests for an injunction[69] and enter an order that (1) bars the Government from collecting, as part of the NSA's Bulk Telephony Metadata Program, any telephony metadata associated with their personal Verizon accounts and (2) requires the Government to destroy any such metadata in its possession that was collected through the bulk collection program.[70]

However, in light of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will stay my order pending appeal.[71] In doing so, I hereby give the Government fair notice that should my ruling be upheld, this order will go into effect forthwith. Accordingly, I fully expect that during the appellate process, which will consume at least the next six months, the Government will take whatever steps necessary to prepare itself to comply with this order when, and if, it is

[69] For reasons stated at the outset, this relief is limited to *Klayman I* plaintiffs Larry Klayman and Charles Strange. I will deny Mary Ann Strange's motion and the motion in *Klayman II*.

[70] Although it is true that granting plaintiffs the relief they request will force the Government to identify plaintiffs' phone numbers and metadata records, and then subject them to otherwise unnecessary individual scrutiny, *see* Shea Decl. ¶ 64, that is the only way to remedy the constitutional violations that plaintiffs are substantially likely to prove on the merits.

[71] *See, e.g.*, *Doe v. Gonzales*, 386 F. Supp. 2d 66, 83 (D. Conn. 2005) ("The court finds that it is appropriate to grant a brief stay of a preliminary injunction in order to permit the Court of Appeals an opportunity to consider an application for a stay pending an expedited appeal."); *Luevano v. Horner*, No. 79-0271, 1988 WL 147603, at *8 (D.D.C. June 27, 1988) ("[T]he Court will enter the injunctive relief that has been requested by plaintiffs but will, *sua sponte*, stay the effect of that injunction pending the outcome of the appeal in [a related case]. In this way, the interests of justice will best be served.").

upheld. Suffice it to say, requesting further time to comply with this order months from now will not be well received and could result in collateral sanctions.

RICHARD J. LEON
United States District Judge

366

JUDGMENT OF THE COURT (Grand Chamber)

13 May 2014 (*)

(Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8)

In Case C-131/12,

REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012, in the proceedings

Google Spain SL,

Google Inc.

v

Agencia Española de Protección de Datos (AEPD),

Mario Costeja González,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, M. Ilešič (Rapporteur), L. Bay Larsen, T. von Danwitz, M. Safjan, Presidents of Chambers, J. Malenovský, E. Levits, A. Ó Caoimh, A. Arabadjiev, M. Berger, A. Prechal and E. Jarašiūnas Judges,

Advocate General: N. Jääskinen,

Registrar: M. Ferreira, Principal Administrator,

having regard to the written procedure and further to the hearing on 26 February 2013,

after considering the observations submitted on behalf of:

- Google Spain SL and Google Inc., by F. González Díaz, J. Baño Fos and B. Holles, abogados,
- Mr Costeja González, by J. Muñoz Rodríguez, abogado,
- the Spanish Government, by A. Rubio González, acting as Agent,
- the Greek Government, by E.-M. Mamouna and K. Boskovits, acting as Agents,
- the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,

– the Austrian Government, by G. Kunnert and C. Pesendorfer, acting as Agents,

– the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,

– the European Commission, by I. Martínez del Peral and B. Martenczuk, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 25 June 2013,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 2(b) and (d), Article 4(1)(a) and (c), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) and of Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The request has been made in proceedings between, on the one hand, Google Spain SL ('Google Spain') and Google Inc. and, on the other, the Agencia Española de Protección de Datos (Spanish Data Protection Agency; 'the AEPD') and Mr Costeja González concerning a decision by the AEPD upholding the complaint lodged by Mr Costeja González against those two companies and ordering Google Inc. to adopt the measures necessary to withdraw personal data relating to Mr Costeja González from its index and to prevent access to the data in the future.

Legal context

European Union law

3 Directive 95/46 which, according to Article 1, has the object of protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and of removing obstacles to the free flow of such data, states in recitals 2, 10, 18 to 20 and 25 in its preamble:

'(2) ... data-processing systems are designed to serve man; ... they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to ... the well-being of individuals;

...

(10) ... the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [, signed in Rome on 4 November 1950,] and in the general principles of Community law; ... for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

...

(18) ... in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; ... in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) ... establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; ... the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor in this respect; ... when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) ... the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; ... in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

...

(25) ... the principles of protection must be reflected, on the one hand, in the obligations imposed on persons ... responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances'.

4 Article 2 of Directive 95/46 states that '[f]or the purposes of this Directive:

(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

...

(d) "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

...'

5 Article 3 of Directive 95/46, entitled 'Scope', states in paragraph 1:

'This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.'

6 Article 4 of Directive 95/46, entitled 'National law applicable', provides:

'1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.'

7 In Section I (entitled 'Principles relating to data quality') of Chapter II of Directive 95/46, Article 6 is worded as follows:

'1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer

periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.'

8 In Section II (entitled 'Criteria for making data processing legitimate') of Chapter II of Directive 95/46, Article 7 provides:

'Member States shall provide that personal data may be processed only if:

...

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

9 Article 9 of Directive 95/46, entitled 'Processing of personal data and freedom of expression', provides:

'Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.'

10 Article 12 of Directive 95/46, entitled 'Rights of access', provides:

'Member States shall guarantee every data subject the right to obtain from the controller:

...

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

...'

11 Article 14 of Directive 95/46, entitled 'The data subject's right to object', provides:

'Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

...'

12 Article 28 of Directive 95/46, entitled 'Supervisory authority', is worded as follows:

'1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

...

3. Each authority shall in particular be endowed with:

– investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

– effective powers of intervention, such as, for example, that ... of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing ...

– ...

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

...

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

...'

Spanish law

13 Directive 95/46 was transposed into Spanish Law by Organic Law No 15/1999 of 13 December 1999 on the protection of personal data (BOE No 298 of 14 December 1999, p. 43088).

The dispute in the main proceedings and the questions referred for a preliminary ruling

14 On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) ('La Vanguardia'), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

15 By that complaint, Mr Costeja González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, he requested that

Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. Mr Costeja González stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.

16 By decision of 30 July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.

17 On the other hand, the complaint was upheld in so far as it was directed against Google Spain and Google Inc. The AEPD considered in this regard that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where they appear, including when retention of the information on that site is justified by a statutory provision.

18 Google Spain and Google Inc. brought separate actions against that decision before the Audiencia Nacional (National High Court). The Audiencia Nacional joined the actions.

19 That court states in the order for reference that the actions raise the question of what obligations are owed by operators of search engines to protect personal data of persons concerned who do not wish that certain information, which is published on third parties' websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to internet users indefinitely. The answer to that question depends on the way in which Directive 95/46 must be interpreted in the context of these technologies, which appeared after the directive's publication.

20 In those circumstances, the Audiencia Nacional decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. With regard to the territorial application of Directive [95/46] and, consequently, of the Spanish data protection legislation:

(a) must it be considered that an "establishment", within the meaning of Article 4(1)(a) of Directive 95/46, exists when any one or more of the following circumstances arise:

– when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State,

or

– when the parent company designates a subsidiary located in that Member State as

its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking,

or

– when the office or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily?

(b) Must Article 4(1)(c) of Directive 95/46 be interpreted as meaning that there is "use of equipment ... situated on the territory of the said Member State":

– when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State,

or

– when it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State?

(c) Is it possible to regard as a use of equipment, in the terms of Article 4(1)(c) of Directive 95/46, the temporary storage of the information indexed by internet search engines? If the answer to that question is affirmative, can it be considered that that connecting factor is present when the undertaking refuses to disclose the place where it stores those indexes, invoking reasons of competition?

(d) Regardless of the answers to the foregoing questions and particularly in the event that the Court ... considers that the connecting factors referred to in Article 4 of [Directive 95/46] are not present:

must Directive 95/46 ... be applied, in the light of Article 8 of the [Charter], in the Member State where the centre of gravity of the conflict is located and more effective protection of the rights of ... Union citizens is possible?

2. As regards the activity of search engines as providers of content in relation to Directive 95/46 ...:

(a) in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of "processing of ... data" used in Article 2(b) of Directive 95/46?

(b) If the answer to the foregoing question is affirmative, and once again in relation to an activity like the one described:

must Article 2(d) of Directive 95/46 be interpreted as meaning that the undertaking managing [Google Search] is to be regarded as the "controller" of the personal data contained in the web pages that it indexes?

(c) In the event that the answer to the foregoing question is affirmative:

may the [AEPD], protecting the rights embodied in [Article] 12(b) and [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, directly impose on [Google Search] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located?

(d) In the event that the answer to the foregoing question is affirmative:

would the obligation of search engines to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?

3. Regarding the scope of the right of erasure and/or the right to object, in relation to the "derecho al olvido" (the "right to be forgotten"), the following question is asked:

must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?'

Consideration of the questions referred

Question 2(a) and (b), concerning the material scope of Directive 95/46

21 By Question 2(a) and (b), which it is appropriate to examine first, the referring court asks, in essence, whether Article 2(b) of Directive 95/46 is to be interpreted as meaning that the activity of a search engine as a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of that provision when that information contains personal data. If the answer is in the affirmative, the referring court seeks to ascertain furthermore whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the 'controller' in respect of that processing of the personal data, within the meaning of that provision.

22 According to Google Spain and Google Inc., the activity of search engines cannot be regarded as processing of the data which appear on third parties' web pages displayed in the list of search results, given that search engines process all the information available on the internet without effecting a selection between personal data and other information. Furthermore, even if that activity must be classified as 'data processing', the operator of a search engine cannot be regarded as a 'controller' in respect of that processing since it has no knowledge of those data and does not exercise control over the data.

23 On the other hand, Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the European Commission consider that that activity quite clearly involves 'data processing'

within the meaning of Directive 95/46, which is distinct from the data processing by the publishers of websites and pursues different objectives from such processing. The operator of a search engine is the 'controller' in respect of the data processing carried out by it since it is the operator that determines the purposes and means of that processing.

24 In the Greek Government's submission, the activity in question constitutes such 'processing', but inasmuch as search engines serve merely as intermediaries, the undertakings which operate them cannot be regarded as 'controllers', except where they store data in an 'intermediate memory' or 'cache memory' for a period which exceeds that which is technically necessary.

25 Article 2(b) of Directive 95/46 defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

26 As regards in particular the internet, the Court has already had occasion to state that the operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46 (see Case C-101/01 *Lindqvist* EU:C:2003:596, paragraph 25).

27 So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data' within the meaning of Article 2(a) of that directive.

28 Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.

29 Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine.

30 The Court has already held that the operations referred to in Article 2(b) of Directive 95/46 must also be classified as such processing where they exclusively concern material that has already been published in unaltered form in the media. It has indeed observed in that regard that a general derogation from the application of Directive 95/46 in such a case would largely deprive the directive of its effect (see, to this effect, Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* EU:C:2008:727, paragraphs 48 and 49).

31 Furthermore, it follows from the definition contained in Article 2(b) of Directive 95/46 that, whilst the alteration of personal data indeed constitutes processing within the meaning of the directive, the other operations which are mentioned there do not, on the other hand, in any way require that the personal data be altered.

32 As to the question whether the operator of a search engine must be regarded as the 'controller' in respect of the processing of personal data that is carried out by that engine in the context of an activity such as that at issue in the main proceedings, it should be recalled that Article 2(d) of Directive 95/46 defines 'controller' as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'.

33 It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).

34 Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.

35 In this connection, it should be pointed out that the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page.

36 Moreover, it is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published.

37 Also, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users' access to that information may, when users carry out their search on the basis of an individual's name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject.

38 Inasmuch as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.

39 Finally, the fact that publishers of websites have the option of indicating to operators of search engines, by means in particular of exclusion protocols such as 'robot.txt' or codes such as 'noindex' or 'noarchive', that they wish specific information published on their site to be wholly or partially excluded from the search engines' automatic indexes does not mean that, if publishers of websites do not so indicate, the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity.

40 That fact does not alter the position that the purposes and means of that processing are determined by the operator of the search engine. Furthermore, even if that option for publishers of websites were to mean that they determine the means of that processing jointly with that operator, this finding

would not remove any of the latter's responsibility as Article 2(d) of Directive 95/46 expressly provides that that determination may be made 'alone or jointly with others'.

41 It follows from all the foregoing considerations that the answer to Question 2(a) and (b) is that Article 2(b) and (d) of Directive 95/46 are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).

Question 1(a) to (d), concerning the territorial scope of Directive 95/46

42 By Question 1(a) to (d), the referring court seeks to establish whether it is possible to apply the national legislation transposing Directive 95/46 in circumstances such as those at issue in the main proceedings.

43 In this respect, the referring court has established the following facts:

- Google Search is offered worldwide through the website 'www.google.com'. In numerous States, a local version adapted to the national language exists. The version of Google Search in Spanish is offered through the website 'www.google.es', which has been registered since 16 September 2003. Google Search is one of the most used search engines in Spain.

- Google Search is operated by Google Inc., which is the parent company of the Google Group and has its seat in the United States.

- Google Search indexes websites throughout the world, including websites located in Spain. The information indexed by its 'web crawlers' or robots, that is to say, computer programmes used to locate and sweep up the content of web pages methodically and automatically, is stored temporarily on servers whose State of location is unknown, that being kept secret for reasons of competition.

- Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms, for undertakings which wish to use that tool in order to offer their goods or services to the internet users.

- The Google group has recourse to its subsidiary Google Spain for promoting the sale of advertising space generated on the website 'www.google.com'. Google Spain, which was established on 3 September 2003 and possesses separate legal personality, has its seat in Madrid (Spain). Its activities are targeted essentially at undertakings based in Spain, acting as a commercial agent for the Google group in that Member State. Its objects are to promote, facilitate and effect the sale of on-line advertising products and services to third parties and the marketing of that advertising.

- Google Inc. designated Google Spain as the controller, in Spain, in respect of two filing systems registered by Google Inc. with the AEPD; those filing systems were intended to contain the personal data of the customers who had concluded contracts for advertising services with Google Inc.

44 Specifically, the main issues raised by the referring court concern the notion of 'establishment', within the meaning of Article 4(1)(a) of Directive 95/46, and of 'use of equipment situated on the territory of the said Member State', within the meaning of Article 4(1)(c).

Question 1(a)

45 By Question 1(a), the referring court asks, in essence, whether Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when one or more of the following three conditions are met:

- the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State, or

- the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking, or

- the branch or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to protection of personal data, even where such collaboration is engaged in voluntarily.

46 So far as concerns the first of those three conditions, the referring court states that Google Search is operated and managed by Google Inc. and that it has not been established that Google Spain carries out in Spain an activity directly linked to the indexing or storage of information or data contained on third parties' websites. Nevertheless, according to the referring court, the promotion and sale of advertising space, which Google Spain attends to in respect of Spain, constitutes the bulk of the Google group's commercial activity and may be regarded as closely linked to Google Search.

47 Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the Commission submit that, in the light of the inextricable link between the activity of the search engine operated by Google Inc. and the activity of Google Spain, the latter must be regarded as an establishment of the former and the processing of personal data is carried out in context of the activities of that establishment. On the other hand, according to Google Spain, Google Inc. and the Greek Government, Article 4(1)(a) of Directive 95/46 is not applicable in the case of the first of the three conditions listed by the referring court.

48 In this regard, it is to be noted first of all that recital 19 in the preamble to Directive 95/46 states that 'establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements' and that 'the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor'.

49 It is not disputed that Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain. As it moreover has separate legal personality, it constitutes a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of Article 4(1)(a) of Directive 95/46.

50 In order to satisfy the criterion laid down in that provision, it is also necessary that the processing of personal data by the controller be 'carried out in the context of the activities' of an establishment of the controller on the territory of a Member State.

51 Google Spain and Google Inc. dispute that this is the case since the processing of personal data at issue in the main proceedings is carried out exclusively by Google Inc., which operates Google Search without any intervention on the part of Google Spain; the latter's activity is limited to providing support to the Google group's advertising activity which is separate from its search engine service.

52 Nevertheless, as the Spanish Government and the Commission in particular have pointed out, Article 4(1)(a) of Directive 95/46 does not require the processing of personal data in question to be carried out 'by' the establishment concerned itself, but only that it be carried out 'in the context of the activities' of the establishment.

53 Furthermore, in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively (see, by analogy, Case C-324/09 *L'Oréal and Others* EU:C:2011:474, paragraphs 62 and 63).

54 It is to be noted in this context that it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope.

55 In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.

56 In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.

57 As has been stated in paragraphs 26 to 28 of the present judgment, the very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory.

58 That being so, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure (see, by analogy, *L'Oréal and Others* EU:C:2011:474, paragraphs 62 and 63), in particular their right to privacy, with respect to the processing of personal data, a right to which the directive accords special importance as is confirmed in particular by Article 1(1) thereof and recitals 2 and 10 in its preamble (see, to this effect, Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 70; Case C-553/07 *Rijkeboer*

EU:C:2009:293, paragraph 47; and Case C-473/12 *IPI* EU:C:2013:715, paragraph 28 and the case-law cited).

59 Since the first of the three conditions listed by the referring court suffices by itself for it to be concluded that an establishment such as Google Spain satisfies the criterion laid down in Article 4(1)(a) of Directive 95/46, it is unnecessary to examine the other two conditions.

60 It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

Question 1(b) to (d)

61 In view of the answer given to Question 1(a), there is no need to answer Question 1(b) to (d).

Question 2(c) and (d), concerning the extent of the responsibility of the operator of a search engine under Directive 95/46

62 By Question 2(c) and (d), the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

63 Google Spain and Google Inc. submit that, by virtue of the principle of proportionality, any request seeking the removal of information must be addressed to the publisher of the website concerned because it is he who takes the responsibility for making the information public, who is in a position to appraise the lawfulness of that publication and who has available to him the most effective and least restrictive means of making the information inaccessible. Furthermore, to require the operator of a search engine to withdraw information published on the internet from its indexes would take insufficient account of the fundamental rights of publishers of websites, of other internet users and of that operator itself.

64 According to the Austrian Government, a national supervisory authority may order such an operator to erase information published by third parties from its filing systems only if the data in question have been found previously to be unlawful or incorrect or if the data subject has made a successful objection to the publisher of the website on which that information was published.

65 Mr Costeja González, the Spanish, Italian and Polish Governments and the Commission submit that the national authority may directly order the operator of a search engine to withdraw from its indexes and intermediate memory information containing personal data that has been published by third parties, without having to approach beforehand or simultaneously the publisher of the web page on which that information appears. Furthermore, according to Mr Costeja González, the Spanish and Italian Governments and the Commission, the fact that the information has been published lawfully and that it still appears on the original web page has no effect on the obligations

of that operator under Directive 95/46. On the other hand, according to the Polish Government that fact is such as to release the operator from its obligations.

66 First of all, it should be remembered that, as is apparent from Article 1 and recital 10 in the preamble, Directive 95/46 seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (see, to this effect, *IPI* EU:C:2013:715, paragraph 28).

67 According to recital 25 in the preamble to Directive 95/46, the principles of protection laid down by the directive are reflected, on the one hand, in the obligations imposed on persons responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals whose data are the subject of processing to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.

68 The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter (see, in particular, Case C-274/99 P *Connolly* v *Commission* EU:C:2001:127, paragraph 37, and *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 68).

69 Article 7 of the Charter guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data. Article 8(2) and (3) specify that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that everyone has the right of access to data which have been collected concerning him or her and the right to have the data rectified, and that compliance with these rules is to be subject to control by an independent authority. Those requirements are implemented inter alia by Articles 6, 7, 12, 14 and 28 of Directive 95/46.

70 Article 12(b) of Directive 95/46 provides that Member States are to guarantee every data subject the right to obtain from the controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data. As this final point relating to the case where certain requirements referred to in Article 6(1)(d) of Directive 95/46 are not observed is stated by way of example and is not exhaustive, it follows that non-compliant nature of the processing, which is capable of conferring upon the data subject the right guaranteed in Article 12(b) of the directive, may also arise from non-observance of the other conditions of lawfulness that are imposed by the directive upon the processing of personal data.

71 In this connection, it should be noted that, subject to the exceptions permitted under Article 13 of Directive 95/46, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (see *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 65; Joined Cases C-468/10 and C-469/10 *ASNEF and FECEMD* EU:C:2011:777, paragraph 26; and Case C-342/12 *Worten* EU:C:2013:355, paragraph 33).

72 Under Article 6 of Directive 95/46 and without prejudice to specific provisions that the Member States may lay down in respect of processing for historical, statistical or scientific purposes, the controller has the task of ensuring that personal data are processed 'fairly and lawfully', that they are 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes', that they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed', that they are 'accurate and, where necessary, kept up to date' and, finally, that they are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'. In this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified.

73 As regards legitimation, under Article 7 of Directive 95/46, of processing such as that at issue in the main proceedings carried out by the operator of a search engine, that processing is capable of being covered by the ground in Article 7(f).

74 This provision permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy with respect to the processing of personal data — which require protection under Article 1(1) of the directive. Application of Article 7(f) thus necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter (see *ASNEF and FECEMD*, EU:C:2011:777, paragraphs 38 and 40).

75 Whilst the question whether the processing complies with Articles 6 and 7(f) of Directive 95/46 may be determined in the context of a request as provided for in Article 12(b) of the directive, the data subject may, in addition, rely in certain conditions on the right to object laid down in subparagraph (a) of the first paragraph of Article 14 of the directive.

76 Under subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, Member States are to grant the data subject the right, at least in the cases referred to in Article 7(e) and (f) of the directive, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. The balancing to be carried out under subparagraph (a) of the first paragraph of Article 14 thus enables account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

77 Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.

78 In this connection, it is to be noted that it is clear from Article 28(3) and (4) of Directive 95/46 that each supervisory authority is to hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data and that it has investigative powers and effective powers of intervention enabling it to order in particular the blocking, erasure or destruction of data or to impose a temporary or definitive ban on such processing.

79 It is in the light of those considerations that it is necessary to interpret and apply the provisions of Directive 95/46 governing the data subject's rights when he lodges with the supervisory authority or judicial authority a request such as that at issue in the main proceedings.

80 It must be pointed out at the outset that, as has been found in paragraphs 36 to 38 of the present judgment, processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10 *eDate Advertising and Others* EU:C:2011:685, paragraph 45).

81 In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing. However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

82 Following the appraisal of the conditions for the application of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 which is to be carried out when a request such as that at issue in the main proceedings is lodged with it, the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties containing information relating to that person, without an order to that effect presupposing the previous or simultaneous removal of that name and information — of the publisher's own accord or following an order of one of those authorities — from the web page on which they were published.

83 As has been established in paragraphs 35 to 38 of the present judgment, inasmuch as the data processing carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites and affects the data subject's fundamental rights additionally, the operator of the search engine as the controller in respect of that processing must ensure, within the framework of its responsibilities, powers and capabilities, that that processing meets the requirements of Directive 95/46, in order that the guarantees laid down by the directive may have full effect.

84 Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to

obtain first or in parallel the erasure of the information relating to them from the publishers of websites.

85 Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. It cannot therefore be ruled out that in certain circumstances the data subject is capable of exercising the rights referred to in Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 against that operator but not against the publisher of the web page.

86 Finally, it must be stated that not only does the ground, under Article 7 of Directive 95/46, justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same.

87 Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page.

88 In the light of all the foregoing considerations, the answer to Question 2(c) and (d) is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

Question 3, concerning the scope of the data subject's rights guaranteed by Directive 95/46

89 By Question 3, the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as enabling the data subject to require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be 'forgotten' after a certain time.

90 Google Spain, Google Inc., the Greek, Austrian and Polish Governments and the Commission consider that this question should be answered in the negative. Google Spain, Google Inc., the Polish Government and the Commission submit in this regard that Article 12(b) and subparagraph

(a) of the first paragraph of Article 14 of Directive 95/46 confer rights upon data subjects only if the processing in question is incompatible with the directive or on compelling legitimate grounds relating to their particular situation, and not merely because they consider that that processing may be prejudicial to them or they wish that the data being processed sink into oblivion. The Greek and Austrian Governments submit that the data subject must approach the publisher of the website concerned.

91 According to Mr Costeja González and the Spanish and Italian Governments, the data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy — which encompass the 'right to be forgotten' — override the legitimate interests of the operator of the search engine and the general interest in freedom of information.

92 As regards Article 12(b) of Directive 95/46, the application of which is subject to the condition that the processing of personal data be incompatible with the directive, it should be recalled that, as has been noted in paragraph 72 of the present judgment, such incompatibility may result not only from the fact that such data are inaccurate but, in particular, also from the fact that they are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.

93 It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.

94 Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.

95 So far as concerns requests as provided for by Article 12(b) of Directive 95/46 founded on alleged non-compliance with the conditions laid down in Article 7(f) of the directive and requests under subparagraph (a) of the first paragraph of Article 14 of the directive, it must be pointed out that in each case the processing of personal data must be authorised under Article 7 for the entire period during which it is carried out.

96 In the light of the foregoing, when appraising such requests made in order to oppose processing such as that at issue in the main proceedings, it should in particular be examined whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. In this connection, it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject.

97 As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, as follows in particular from paragraph 81 of the present judgment, that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.

98 As regards a situation such as that at issue in the main proceedings, which concerns the display, in the list of results that the internet user obtains by making a search by means of Google Search on the basis of the data subject's name, of links to pages of the on-line archives of a daily newspaper that contain announcements mentioning the data subject's name and relating to a real-estate auction connected with attachment proceedings for the recovery of social security debts, it should be held that, having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed from the list of results.

99 It follows from the foregoing considerations that the answer to Question 3 is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

Costs

100 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).

2. Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

3. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

4. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

[Signatures]

 388

14-42
ACLU v. Clapper

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2014

(Argued: September 2, 2014 Decided: May 7, 2015)

Docket No. 14-42-cv

AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, NEW YORK CIVIL LIBERTIES UNION, NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs-Appellants,

— v. —

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence, MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service, ASHTON B. CARTER, in his official capacity as Secretary of Defense, LORETTA E. LYNCH, in her official capacity as Attorney General of the United States, and JAMES B. COMEY, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants-Appellees.[*]

[*] The Clerk of Court is respectfully directed to amend the official caption in this case to conform with the caption above. See Fed. R. App. P. 43(c)(2).

Before:

SACK and LYNCH, *Circuit Judges*, and BRODERICK, *District Judge*.**

Plaintiffs-appellants American Civil Liberties Union and American Civil Liberties Union Foundation, and New York Civil Liberties Union and New York Civil Liberties Union Foundation, appeal from a decision of the United States District Court for the Southern District of New York (William H. Pauley, III, *Judge*) granting defendants-appellees' motion to dismiss and denying plaintiffs-appellants' request for a preliminary injunction. The district court held that § 215 of the PATRIOT Act impliedly precludes judicial review; that plaintiffs-appellants' statutory claims regarding the scope of § 215 would in any event fail on the merits; and that § 215 does not violate the Fourth or First Amendments to the United States Constitution. We disagree in part, and hold that § 215 and the statutory scheme to which it relates do not preclude judicial review, and that the bulk telephone metadata program is not authorized by § 215. We therefore

** The Honorable Vernon S. Broderick, of the United States District Court for the Southern District of New York, sitting by designation.

VACATE the judgment of the district court and REMAND for further proceedings consistent with this opinion.

VACATED AND REMANDED.

Robert D. Sack, *Circuit Judge*, concurs in the opinion of the Court and files a separate concurring opinion.

ALEXANDER ABDO, American Civil Liberties Union Foundation (Jameel Jaffer, Patrick Toomey, Brett Max Kaufman, Catherine Crump, American Civil Liberties Union Foundation, New York, NY; Christopher T. Dunn, Arthur N. Eisenburg, New York Civil Liberties Union Foundation, New York, NY, *on the brief*), New York, NY, *for Plaintiffs-Appellants.*

STUART F. DELERY, Assistant Attorney General, Civil Division, United States Department of Justice (Douglas N. Letter, H. Thomas Byron III, Henry C. Whitaker, Appellate Staff, Civil Division, United States Department of Justice, Washington, DC; Preet Bharara, United States Attorney for the Southern District of New York, New York, NY; David S. Jones, John D. Clopper, Emily E. Daughtry, Assistant United States Attorneys, New York, NY, *on the brief*), Washington, D.C., *for Defendants-Appellees.*

Laura K. Donohue, Georgetown University Law Center, Washington DC, Erwin Chemerinsky, University of California, Irvine School of Law, Irvine, CA, *for Amici Curiae Former Members of the Church Committee and Law Professors in Support of Plaintiffs-Appellants.*

Charles S. Sims, Proskauer Rose LLP, New York, NY, *for Amici Curiae Senator Ron Wyden, Senator Mark Udall, and Senator Martin Heinrich in Support of Plaintiffs-Appellants.*

Cindy Cohn, Mark Rumold, Andrew Crocker, Electronic Frontier Foundation, San Francisco, CA, *for Amici Curiae Experts in Computer and Data Science in Support of Appellants and Reversal.*

John W. Whitehead, Douglas R. McKusick, The Rutherford Institute, Charlottesville, Virginia, Daniel L. Ackman, Law Office of Daniel Ackman, New York, NY, *for Amicus Curiae The Rutherford Institute in Support of Appellants and Reversal.*

Edward J. Davis, Linda Steinman, Lacy H. Koonce, III, Davis Wright Tremaine LLP, New York, NY, *for Amicus Curiae PEN American Center, Inc., in Support of Appellants.*

John Frazer, Law Office of John Frazer, PLLC, Fairfax, VA, *for Amicus Curiae National Rifle Association of America, Inc., in Support of Plaintiffs-Appellants and Supporting Reversal.*

Jonathan Hafetz, Association of the Bar of the City of New York, Gary D. Sesser, Stephen L. Kass, Michael Shapiro, Laura A. Zaccone, Carter Ledyard & Milburn LLP, New York, NY, *for Amicus Curiae Association of the Bar of the City of New York Supporting Plaintiffs-Appellants' Brief.*

GERARD E. LYNCH, *Circuit Judge*:

This appeal concerns the legality of the bulk telephone metadata collection program (the "telephone metadata program"), under which the National Security Agency ("NSA") collects in bulk "on an ongoing daily basis" the metadata associated with telephone calls made by and to Americans, and aggregates those metadata into a repository or data bank that can later be queried. Appellants

challenge the program on statutory and constitutional grounds. Because we find that the program exceeds the scope of what Congress has authorized, we vacate the decision below dismissing the complaint without reaching appellants' constitutional arguments. We affirm the district court's denial of appellants' request for a preliminary injunction.

BACKGROUND

In the early 1970s, in a climate not altogether unlike today's, the intelligence-gathering and surveillance activities of the NSA, the FBI, and the CIA came under public scrutiny. The Supreme Court struck down certain warrantless surveillance procedures that the government had argued were lawful as an exercise of the President's power to protect national security, remarking on "the inherent vagueness of the domestic security concept [and] the necessarily broad and continuing nature of intelligence gathering." United States v. U.S. Dist. Court for the E. Dist. of Mich. (Keith), 407 U.S. 297, 320 (1972). In response to that decision and to allegations that those agencies were abusing their power in order to spy on Americans, the Senate established the Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee") to investigate whether the intelligence agencies had engaged in

unlawful behavior and whether legislation was necessary to govern their activities. The Church Committee expressed concerns that the privacy rights of U.S. citizens had been violated by activities that had been conducted under the rubric of foreign intelligence collection.

The findings of the Church Committee, along with the Supreme Court's decision in Keith and the allegations of abuse by the intelligence agencies, prompted Congress in 1978 to enact comprehensive legislation aimed at curtailing abuses and delineating the procedures to be employed in conducting surveillance in foreign intelligence investigations. That legislation, the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801 et seq.), established a special court, the Foreign Intelligence Surveillance Court ("FISC"), to review the government's applications for orders permitting electronic surveillance. See 50 U.S.C. § 1803. Unlike ordinary Article III courts, the FISC conducts its usually ex parte proceedings in secret; its decisions are not, in the ordinary course, disseminated publicly. Id. § 1803(c).

We are faced today with a controversy similar to that which led to the Keith decision and the enactment of FISA. We must confront the question

whether a surveillance program that the government has put in place to protect national security is lawful. That program involves the bulk collection by the government of telephone metadata created by telephone companies in the normal course of their business but now explicitly required by the government to be turned over in bulk on an ongoing basis. As in the 1970s, the revelation of this program has generated considerable public attention and concern about the intrusion of government into private matters. As in that era, as well, the nation faces serious threats to national security, including the threat of foreign-generated acts of terrorism against the United States. Now, as then, Congress is tasked in the first instance with achieving the right balance between these often-competing concerns. To do so, Congress has amended FISA, most significantly, after the terrorist attacks of September 11, 2001, in the PATRIOT Act. See USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). The government argues that § 215 of that Act authorizes the telephone metadata program. See id. § 215, 115 Stat. at 287 (codified as amended at 50 U.S.C. § 1861).

I. Telephone Metadata

Before proceeding to explore the details of § 215 of the PATRIOT Act, we pause to define "telephone metadata," in order to clarify the type of information

that the government argues § 215 authorizes it to collect in bulk. Unlike what is gleaned from the more traditional investigative practice of wiretapping, telephone metadata do not include the voice content of telephone conversations. Rather, they include details about telephone calls, including, for example, the length of a call, the phone number from which the call was made, and the phone number called. Metadata can also reveal the user or device making or receiving a call through unique "identity numbers" associated with the equipment (although the government maintains that the information collected does not include information about the identities or names of individuals), and provide information about the routing of a call through the telephone network, which can sometimes (although not always) convey information about a caller's general location. According to the government, the metadata it collects do not include cell site locational information, which provides a more precise indication of a caller's location than call-routing information does.

That telephone metadata do not directly reveal the content of telephone calls, however, does not vitiate the privacy concerns arising out of the government's bulk collection of such data. Appellants and amici take pains to emphasize the startling amount of detailed information metadata can reveal –

"information that could traditionally only be obtained by examining the contents of communications" and that is therefore "often a proxy for content." Joint App'x 50 (Declaration of Professor Edward W. Felten). For example, a call to a single-purpose telephone number such as a "hotline" might reveal that an individual is: a victim of domestic violence or rape; a veteran; suffering from an addiction of one type or another; contemplating suicide; or reporting a crime. Metadata can reveal civil, political, or religious affiliations; they can also reveal an individual's social status, or whether and when he or she is involved in intimate relationships.[1]

---

[1] A report of a recent study in *Science* magazine revealed how much information can be gleaned from credit card metadata. In the study, which used three months of anonymous credit card records for 1.1 million people, scientists were able to reidentify 90% of the individuals where they had only four additional "spatiotemporal points" of information – for example, information that an individual went to one particular store on four specific days. Such information could be gathered from sources as accessible as a "tweet" from that individual. Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex "Sandy" Pentland, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, Science, Jan. 30, 2015, at 536. The study's authors concluded that, in the context of most large-scale metadata sets, it would not be difficult to reidentify individuals even if the data were anonymized. Id. at 539. While credit card data differ in important ways from telephone data, the study illustrates the ways in which metadata can be used by sophisticated investigators to deduce significant private information about individuals.

We recognize that metadata exist in more traditional formats, too, and that law enforcement and others have always been able to utilize metadata for investigative purposes. For example, just as telephone metadata may reveal the charitable organizations that an individual supports, observation of the outside of an envelope sent at the end of the year through the United States Postal Service to such an organization might well permit similar inferences, without requiring an examination of the envelope's contents. But the structured format of telephone and other technology-related metadata, and the vast new technological capacity for large-scale and automated review and analysis, distinguish the type of metadata at issue here from more traditional forms. The more metadata the government collects and analyzes, furthermore, the greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals. Finally, as appellants and amici point out, in today's technologically based world, it is virtually impossible for an ordinary citizen to avoid creating metadata about himself on a regular basis simply by conducting his ordinary affairs.

II. Section 215

The original version of § 215, which pre-dated the PATRIOT Act, allowed

the Director of the FBI or his designee to obtain orders from the FISC authorizing common carriers, among others, to provide to the government certain business records for the purpose of foreign intelligence and international terrorism investigations where there existed "specific and articulable facts giving reason to believe that the person to whom the records pertain [wa]s a foreign power or an agent of a foreign power." That provision was enacted in 1998 as an amendment to FISA. See Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410-11 (1998). The PATRIOT Act substantially revised § 215 to provide for the production not only of "business records" but also of "any tangible things," and to eliminate the restrictions on the types of businesses such orders can reach. See USA PATRIOT ACT of 2001, Pub. L. No. 107-56, § 215. As subsequently amended by successor bills to the PATRIOT Act, the current version of § 215 allows the Director of the FBI or his designee to

> make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

50 U.S.C. § 1861(a)(1). In its current form, the provision requires such an application to include

> a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

Id. § 1861(b)(2)(A). Such an order "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." Id. § 1861(c)(2)(D). Finally, the statute requires the Attorney General to "adopt specific minimization procedures governing the retention and dissemination by the [FBI] of any tangible things, or information therein, received by the [FBI] in response to an order under this subchapter." Id. § 1861(g)(1). Because § 215 contained a "sunset" provision from its inception, originally terminating its authority on December 31, 2005, it has required subsequent renewal. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 224, 115 Stat. at 295.

Congress has renewed § 215 seven times, most recently in 2011, at which time it was amended to expire on June 1, 2015. See PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011).

III. The Telephone Metadata Program

Americans first learned about the telephone metadata program that appellants now challenge on June 5, 2013, when the British newspaper *The Guardian* published a FISC order leaked by former government contractor Edward Snowden. The order directed Verizon Business Network Services, Inc. ("Verizon"), a telephone company, to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From Verizon Bus. Network Servs., Inc., ex rel. MCI Commc'n Servs., Inc., d/b/a Verizon Bus. Servs. ("Verizon Secondary Order"), No. BR 13-80, slip op. at 2 (F.I.S.C. Apr. 25, 2013). The order thus requires Verizon to produce call detail records, every day, on *all* telephone calls made through its systems or using its services where one or both ends of the call are located in the United States.

 401

After the order was published, the government acknowledged that it was part of a broader program of bulk collection of telephone metadata from other telecommunications providers carried out pursuant to § 215. It is now undisputed that the government has been collecting telephone metadata information in bulk under § 215 since at least May 2006, when the FISC first authorized it to do so in a "Primary Order" describing the "tangible things" to be produced as "all call-detail records or 'telephony metadata' created by [redacted] . . . , includ[ing] comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number[s], communications device identifier[s], etc.), trunk identifier, and time and duration of call." In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [Redacted] ("2006 Primary Order"), No. BR 06-05, slip op. at 2 (F.I.S.C. May 24, 2006), http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf.

That order specified that the items were to be produced to the NSA; that there were "reasonable grounds to believe the tangible things sought [were] relevant to authorized investigations . . . to protect against international

terrorism"; and that the items sought "could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." Id. at 3. The order required its recipient, upon receiving the "appropriate secondary order,"[2] to "continue production on an ongoing daily basis . . . for the duration of th[e] order" and contemplated creation of a "data archive" that would only be accessed "when NSA has identified a known telephone number for which . . . there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [Redacted]"– presumably, with terrorist activity or a specific terrorist organization. Id. at 4-5. The order also states that the NSA "exclusively will operate" the network on which the metadata are stored and processed. Id. at 5.

The government has disclosed additional FISC orders reauthorizing the program. FISC orders must be renewed every 90 days, and the program has therefore been renewed 41 times since May 2006. Most recently, the program

[2] The order published in *The Guardian* and served on Verizon was one such "Secondary Order."

was reauthorized by the FISC on February 26, 2015; that authorization expires on June 1, 2015. See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [Redacted], No. BR 15-24 (F.I.S.C. Feb. 26, 2015), http://www.dni.gov/files/documents/0311/BR%2015-24%20Primary%20Order%20-%20Redacted.pdf.

The government disputes appellants' characterization of the program as collecting "virtually all telephony metadata" associated with calls made or received in the United States, but declines to elaborate on the scope of the program or specify how the program falls short of that description. It is unclear, however, in what way appellants' characterization of the program can be faulted. On its face, the Verizon order requires the production of "*all* call detail records or 'telephony metadata'" relating to Verizon communications within the United States or between the United States and abroad. Verizon Secondary Order 2 (emphasis added). The Verizon order and the Primary Order described above reveal that the metadata collected include "comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment

404

Identity (IMEI) number, etc.), trunk identifier,[3] telephone calling card numbers, and time and duration of call." Verizon Secondary Order 2; see also 2006 Primary Order 2. The government does not suggest that Verizon is the only telephone service provider subject to such an order; indeed, it does not seriously dispute appellants' contention that all significant service providers in the United States are subject to similar orders.

The government explains that it uses the bulk metadata collected pursuant to these orders by making "queries" using metadata "identifiers" (also referred to as "selectors"), or particular phone numbers that it believes, based on "reasonable articulable suspicion," to be associated with a foreign terrorist organization. Joint App'x 264 (Declaration of Teresa H. Shea). The identifier is used as a "seed" to search across the government's database; the search results yield phone numbers, and the metadata associated with them, that have been in contact with the seed. Id. That step is referred to as the first "hop." The NSA can then also search for the numbers, and associated metadata, that have been in contact with the numbers resulting from the first search – conducting a second

[3] A "trunk identifier" provides information regarding how a call is routed through the telephone network, revealing general information about the parties' locations.

"hop." Id. at 265. Until recently, the program allowed for another iteration of the process, such that a third "hop" could be conducted, sweeping in results that include the metadata of, essentially, the contacts of contacts of contacts of the original "seed." Id. The government asserts that it does not conduct any general "browsing" of the data. Id. at 263-65.

Section 215 requires that the Attorney General adopt "specific minimization procedures governing the retention and dissemination by the [government] of [information] received . . . in response to an order under this subchapter." 50 U.S.C. § 1861(g)(1). The procedures that have been adopted include the requirement that the NSA store the metadata within secure networks; that the metadata not be accessed for any purpose other than what is allowed under the FISC order; that the results of queries not be disseminated outside the NSA except in accordance with the minimization and dissemination requirements of NSA procedures; and that the relevant personnel receive comprehensive training on the minimization procedures and technical controls. Joint App'x 267-69. And as the government points out, the program is subject to oversight by the Department of Justice, the FISC, and Congress. Id. at 269. The minimization procedures require audits and reviews of the program by the

NSA's legal and oversight offices, the Office of the Inspector General, attorneys from the Department of Justice's National Security Division, and the Office of the Director of National Intelligence. Id. The FISC orders that created the program require the NSA to provide periodic reports to the FISC. Id. at 141. In the event of failures of compliance, reports must be made to the FISC, and, where those failures are significant, to the Intelligence and Judiciary Committees of both houses of Congress. Id. at 269. FISA itself also imposes a system of Congressional oversight, requiring periodic reports on the program from the Attorney General to the House and Senate Intelligence and Judiciary Committees. See 50 U.S.C. §§ 1862, 1871.

Since the existence of the telephone metadata program became public, a number of developments have altered the landscape, at least to some degree, within which we analyze the program. Among the most notable are modifications to the telephone metadata program announced by President Obama in January 2014. President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence. The two immediate modifications that the President ordered, which were subsequently

incorporated in a FISC order sought by government motion, (1) limited the number of "hops" that can be searched to two, rather than three, and (2) required that a FISC judge find that the reasonable articulable suspicion standard has been satisfied before a seed can be queried, rather than (as had previously been the case) allowing designated NSA officials to determine for themselves whether such suspicion existed. Id. Both limitations were approved by the FISC in a February 5, 2014 FISC order. In re Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR-14-01 (F.I.S.C. Feb. 5, 2014), http://www.uscourts.gov/uscourts/courts/fisc/br14-01-order.pdf. These modifications were based in part on the recommendations of the Review Group on Intelligence and Communications Technologies established by the President. See President's Review Grp. on Intelligence and Commc'ns Techs., Liberty and Security in a Changing World: Rep. and Recommendations of the President's Review Grp. on Intelligence and Commc'ns Techs. (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. The Review Group also recommended that the system be modified such that a third party or the private carriers, rather than the government, collect and

retain the bulk metadata. That recommendation, however, has so far not been adopted.

In addition to that group, the Privacy and Civil Liberties Oversight Board ("PCLOB") published a detailed report on the program. The PCLOB is a bipartisan agency within the executive branch that was established in 2007, pursuant to a recommendation from the National Commission on Terrorist Attacks Upon the United States (the "9/11 Commission," established after the September 11, 2001 terrorist attacks to prepare an account of the circumstances surrounding the attacks), in order to monitor the actions taken by the government to protect the nation from terrorism and to ensure that they are appropriately balanced against the need to protect privacy and civil liberties. See Implementing Recommendations of the 9/11 Comm'n Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007). The PCLOB concluded that the program was inconsistent with § 215, violated the Electronic Communications Privacy Act, and implicated privacy and First Amendment concerns. See Privacy and Civil Liberties Oversight Board, Rep. on the Tel. Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (Jan. 23, 2014) ("PCLOB Report"),

https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

Legislation aimed at incorporating stronger protections of individual liberties into the telephone metadata program in a variety of ways (or eliminating it altogether) was introduced in both the House and the Senate during the 113th Congress. See USA FREEDOM Act, H.R. 3361, 113th Cong. (2014); USA FREEDOM Act, S. 2685, 113th Cong. (2014). A modified version of H.R. 3361, which lost the backing of some of the bill's original supporters because it failed to end bulk collection, nevertheless passed the House in May 2014. USA FREEDOM Act, H.R. 3361, 113th Cong. (2014). In November 2014, however, a motion to invoke cloture on the Senate's version of the bill – relatively more robust in terms of privacy protections – failed by a vote of 58-42, thereby preventing the bill from coming up for a vote in the Senate despite the desire of 58 senators to proceed to a vote on the measure. USA FREEDOM Act, S. 2685, 113th Cong. (2014). The current Congress is likewise considering bills aimed at modifying § 215; a bill that would place the bulk metadata collected into the hands of telecommunications providers, to be accessed by the government only with FISC authorization, has been introduced in both the House and the Senate in

recent weeks. See USA FREEDOM Act of 2015, H.R. 2048/S. 1123, 114th Cong. (2015). On April 30, 2015, the bill passed the House Judiciary Committee. See USA FREEDOM Act of 2015, H.R. 2048, 114th Cong. (2015). A vote from the full House on the bill is expected later this month.

Finally, the program has come under scrutiny by Article III courts other than the FISC. In addition to this case, similar cases have been filed around the country challenging the government's bulk collection of telephone metadata. See, e.g., Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014), No. 14-35555 (9th Cir. argued Dec. 8, 2014); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), No. 14-5004 (D.C. Cir. argued Nov. 4, 2014).

IV. Procedural History

On June 11, 2013, the American Civil Liberties Union and American Civil Liberties Union Foundation (collectively, "ACLU") and the New York Civil Liberties Union and New York Civil Liberties Union Foundation (collectively, "NYCLU") – current and former Verizon customers, respectively – sued the government officials responsible for administering the telephone metadata program, challenging the program on both statutory and constitutional grounds and seeking declaratory and injunctive relief. The complaint asks the court to

411

declare that the telephone metadata program exceeds the authority granted by § 215, and also violates the First and Fourth Amendments to the U.S. Constitution. It asks the court to permanently enjoin defendants from continuing the program, and to order defendants to "purge from their possession all of the call records of [p]laintiffs' communications" collected in accordance with the program. Joint App'x 27.

On August 26, 2013, plaintiffs moved for a preliminary injunction barring defendants from collecting their call records under the program, requiring defendants to quarantine all of the call records they had already collected, and prohibiting defendants from using their records to perform queries on any phone number or other identifier associated with plaintiffs. On the same date, the government moved to dismiss the complaint.

On December 27, 2013, the district court granted the government's motion to dismiss and denied plaintiffs' motion for a preliminary injunction. See ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013). Plaintiffs now appeal that decision.

412

DISCUSSION

We review de novo a district court's grant of a motion to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Klein & Co. Futures, Inc. v. Bd. of Trade of City of New York, 464 F.3d 255, 259 (2d Cir. 2006); see also Lotes Co., Ltd. v. Hon Hai Precision Indus. Co., 753 F.3d 395, 403 (2d Cir. 2014). We review a district court's denial of a preliminary injunction for abuse of discretion, see Cent. Rabbinical Cong. of U.S. & Canada v. N.Y.C. Dep't of Health & Mental Hygiene, 763 F.3d 183, 192 (2d Cir. 2014), which occurs when the court's decision either "rests on an error of law . . . or a clearly erroneous factual finding, or . . . its decision – though not necessarily the product of a legal error or a clearly erroneous factual finding – cannot be located within the range of permissible decisions," Vincenty v. Bloomberg, 476 F.3d 74, 83 (2d Cir. 2007).

I. Standing

The district court ruled that appellants had standing to bring this case. Clapper, 959 F. Supp. 2d at 738. The government argues that the district court's ruling was erroneous, contending that appellants lack standing because they have not demonstrated that any of the metadata associated with them have been or will be actually reviewed by the government, and have not otherwise

413

identified an injury that is sufficiently concrete or imminent to confer standing. We recognize that "'[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.'" Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013), quoting DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006) (alteration in original). In order to meet that requirement, plaintiffs must, among other things, establish that they have standing to sue. Raines v. Byrd, 521 U.S. 811, 818 (1997). "Standing under Article III of the Constitution requires that an injury be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010); see also Amnesty Int'l, 133 S. Ct. at 1147 (collecting cases). The Supreme Court has "repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." Amnesty Int'l, 133 S. Ct. at 1147, quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (emphasis in original). We remain mindful that the "'standing inquiry has been especially rigorous when reaching the merits of [a] dispute would force us to decide whether an action taken by one of the

other two branches of the Federal Government was unconstitutional'" and "in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs." Id., quoting Raines, 521 U.S. at 819-20.

Appellants in this case have, despite those substantial hurdles, established standing to sue, as the district court correctly held. Appellants here need not speculate that the government has collected, or may in the future collect, their call records. To the contrary, the government's own orders demonstrate that appellants' call records are indeed among those collected as part of the telephone metadata program. Nor has the government disputed that claim. It argues instead that any alleged injuries here depend on the government's *reviewing* the information collected, and that appellants have not shown anything more than a "speculative prospect that their telephone numbers would ever be used as a selector to query, or be included in the results of queries of, the telephony metadata." Appellees' Br. 22.

But the government's argument misapprehends what is required to establish standing in a case such as this one. Appellants challenge the telephone metadata program as a whole, alleging injury from the very collection of their

telephone metadata. And, as the district court observed, it is not disputed that the government collected telephone metadata associated with the appellants' telephone calls. The Fourth Amendment protects against unreasonable searches *and seizures.* Appellants contend that the collection of their metadata exceeds the scope of what is authorized by § 215 and constitutes a Fourth Amendment search. We think such collection is more appropriately challenged, at least from a standing perspective, as a seizure rather than as a search. Whether or not such claims prevail on the merits, appellants surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them. "[A] violation of the [Fourth] Amendment is fully accomplished at the time of an unreasonable governmental intrusion." United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990) (internal quotation marks omitted). If the telephone metadata program is unlawful, appellants have suffered a concrete and particularized injury fairly traceable to the challenged program and redressable by a favorable ruling.

Amnesty International does not hold otherwise. There, the Supreme Court, reversing our decision, held that respondents had not established standing because they could not show that the government was surveilling them, or that

such surveillance was "certainly impending." 131 S. Ct. at 1148-1150. Instead, the Supreme Court stated that respondents' standing arguments were based on a "speculative chain of possibilities" that required that: respondents' foreign contacts be targeted for surveillance; the surveillance be conducted pursuant to the statute challenged, rather than under some other authority; the FISC approve the surveillance; the government actually intercept the communications of the foreign contacts; and among those intercepted communications be those involving respondents. Id. Because respondents' injury relied on that chain of events actually transpiring, the Court held that the alleged injury was not "fairly traceable" to the statute being challenged. Id. at 1150. As to costs incurred by respondents to avoid surveillance, the Court characterized those costs as "a product of their fear of surveillance" insufficient to confer standing. Id. at 1152.

Here, appellants' alleged injury requires no speculation whatsoever as to how events will unfold under § 215 – appellants' records (among those of numerous others) have been targeted for seizure by the government; the government has used the challenged statute to effect that seizure; the orders have been approved by the FISC; and the records have been collected. Amnesty International's "speculative chain of possibilities" is, in this context, a reality.

417

That case in no way suggested that such data would need to be reviewed or analyzed in order for respondents to suffer injury.

The government also takes issue with the district court's reliance on Amidax Trading Group v. S.W.I.F.T. SCRL, 671 F.3d 140 (2d Cir. 2011). In Amidax, we held that plaintiffs had not established standing to challenge the government's acquisition of financial records from SWIFT, a messaging service that routes financial transactions, via administrative subpoenas issued by the Office of Foreign Asset Control. Id. at 148-49. Because there was insufficient support for the allegation that Amidax's own records were among those handed over to the government, we held that Amidax had not alleged a plausible injury in fact. Id. That case, too, differs from the case at bar, where appellants have presented evidence that their data *are* being collected. To the extent Amidax speaks to the circumstances presented by this case, it supports, albeit in dictum, appellants' position. We noted in Amidax that "[t]o establish an injury in fact – and thus, a personal stake in this litigation – [Amidax] need only establish that its information was obtained by the government." Id. at 147 (second alteration in original). There, too, we viewed the collection of the data in question, if it had in

fact occurred, as an injury sufficient to confer standing, without considering whether such data were likely to be reviewed.

Finally, the government admits that, when it queries its database, its computers search all of the material stored in the database in order to identify records that match the search term. In doing so, it necessarily searches appellants' records electronically, even if such a search does not return appellants' records for close review by a human agent. There is no question that an equivalent manual review of the records, in search of connections to a suspect person or telephone, would confer standing even on the government's analysis. That the search is conducted by a machine might lessen the intrusion, but does not deprive appellants of standing to object to the collection and review of their data.

Appellants likewise have standing to assert a First Amendment violation. Appellants contend that their First Amendment associational rights are being violated, both directly and through a "chilling effect" on clients and donors. The Supreme Court has long recognized that an organization can assert associational privacy rights on behalf of its members, stating that "[i]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in

advocacy may constitute . . . a restraint on freedom of association." NAACP v. Alabama, 357 U.S. 449, 462 (1958). In NAACP, furthermore, the Supreme Court held that the organization "argue[d] . . . appropriately the rights of its members, and that its nexus with them [wa]s sufficient to permit that it act as their representative before this Court." Id. at 458-59. We have similarly stated that a union's "standing to assert the First and Fourteenth Amendment rights of association and privacy of its individual members is beyond dispute." Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor, 667 F.2d 267, 270 (2d Cir. 1981). When the government collects appellants' metadata, appellants' members' interests in keeping their associations and contacts private are implicated, and any potential "chilling effect" is created at that point. Appellants have therefore alleged a concrete, fairly traceable, and redressable injury sufficient to confer standing to assert their First Amendment claims as well.

II. Preclusion and the Administrative Procedure Act

The government next contends that appellants are impliedly precluded from bringing suit to challenge the telephone metadata program on statutory grounds. According to the government, the statutory scheme set out by § 215

limits judicial review of § 215 orders "to the FISC and its specialized mechanism for appellate review," Appellees' Br. 26, and provides for challenges to those orders only by *recipients* of § 215 orders (that is, the communications companies), rather than the targets of such orders, thereby impliedly precluding appellants here from bringing suit in federal court. The government also argues that 18 U.S.C. § 2712 impliedly precludes the relief appellants seek, either independently or in conjunction with the larger statutory framework established by the two provisions.

A. Section 215 and Implied Preclusion

The Administrative Procedure Act ("APA") waives sovereign immunity for suits against the United States for relief other than money damages. Under the APA, "[a] person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof," and can bring suit in an "action in a court of the United States seeking relief other than money damages." 5 U.S.C. § 702. The APA thus establishes a broad right of judicial review of administrative action. The APA does not, however, apply where "statutes preclude judicial review." Id. § 701.

In determining whether judicial review is precluded under a particular statute, we must "begin with the strong presumption that Congress intends judicial review of administrative action. From the beginning 'our cases [have established] that judicial review of a final agency action by an aggrieved person will not be cut off unless there is persuasive reason to believe that such was the purpose of Congress.'" Bowen v. Mich. Acad. of Family Physicians, 476 U.S. 667, 670 (1986), quoting Abbott Labs. v. Gardner, 387 U.S. 136, 140 (1967) (alterations in original). "'[O]nly . . . a showing of clear and convincing evidence of a contrary legislative intent'" can rebut the presumption that Congress intended that an action be subject to judicial review. Bowen, 476 U.S. at 672, quoting Abbott Labs., 387 U.S. at 141. The Supreme Court has emphasized that there is a "heavy burden" on a party that attempts to overcome this presumption. Id. (internal quotation marks omitted).

That burden is, of course, not insurmountable, and "may be overcome by specific language or specific legislative history that is a reliable indicator of congressional intent." Block v. Cmty. Nutrition Inst., 467 U.S. 340, 349 (1984). Such an intent must be "fairly discernible in the statutory scheme," id. at 351 (internal quotation marks omitted), looking to the scheme's "structure . . . , its

objectives, its legislative history, and the nature of the administrative action involved," id. at 345. Importantly, "'where substantial doubt about the congressional intent exists, the general presumption favoring judicial review of administrative action is controlling.'" NRDC v. Johnson, 461 F.3d 164, 172 (2d Cir. 2006), quoting Block, 467 U.S. at 351. Implied preclusion of review is thus disfavored.

The government points to no language in § 215, or in FISA or the PATRIOT Act more generally, that excludes actions taken by executive or administrative officials pursuant to its terms from the presumption of judicial review established by the APA. Rather, it argues that the provision of one mechanism for judicial review, at the behest of parties other than those whose privacy may be compromised by the seizure, impliedly precludes review pursuant to the APA by parties thus aggrieved. To understand that argument, we begin by describing the provision for judicial review on which the government relies.

A recipient of a § 215 order may challenge its legality "by filing a petition with the pool" of FISC judges established by the statute. 50 U.S.C. § 1861(f)(2)(A)(i). That decision can then be appealed to the FISA Court of Review. Id. § 1861(f)(3). The statute also provides that "[a]ny production or

nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect." Id. § 1861(f)(2)(D).

According to the government, those provisions establish a limited and detailed framework that evinces Congressional intent to limit judicial review to the method specified. Both the government and the district court point to the Supreme Court's language in Block that "when a statute provides a detailed mechanism for judicial consideration of particular issues at the behest of particular persons, judicial review of those issues at the behest of other persons may be found to be impliedly precluded." Block, 467 U.S. at 349.

But that is not always the case. The Supreme Court has also noted that "if the express provision of judicial review in one section of a long and complicated statute were alone enough to overcome the APA's presumption of reviewability for all final agency action, it would not be much of a presumption at all." Sackett v. EPA, 132 S. Ct. 1367, 1373 (2012). The question remains whether the government has demonstrated by clear and convincing or "discernible" evidence that Congress intended to preclude review in these particular circumstances.

(1) Secrecy

The government's primary argument in support of preclusion is based on the various secrecy provisions that attach to § 215 orders. For example, § 215 states that "[n]o person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section" unless disclosure is necessary to comply with the order; the disclosure is made to an attorney for advice or assistance in connection with the order; or the disclosure is made to others as permitted by the FBI Director or his designee. 50 U.S.C. § 1861(d)(1). And the statute explicitly lays out various supplemental secrecy procedures accompanying the review process, including the requirements that the records of any such proceedings be "maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence," id. § 1861(f)(4); that "[a]ll petitions . . . be filed under seal," id. § 1861(f)(5); and that, in the case of any government submission that may contain classified information, the court review it ex parte and in camera, id. These secrecy measures, the government argues, are evidence that Congress did

not intend that § 215 orders be reviewable in federal court upon suit by an individual whose metadata are collected.

Upon closer analysis, however, that argument fails. The government has pointed to no affirmative evidence, whether "clear and convincing" or "fairly discernible," that suggests that Congress intended to preclude judicial review. Indeed, the government's argument from secrecy suggests that Congress did not contemplate a situation in which targets of § 215 orders would become aware of those orders on anything resembling the scale that they now have. That revelation, of course, came to pass only because of an unprecedented leak of classified information. That Congress may not have anticipated that individuals like appellants, whose communications were targeted by § 215 orders, would become aware of the orders, and thus be in a position to seek judicial review, is not evidence that Congress affirmatively decided to revoke the right to judicial review otherwise provided by the APA in the event the orders *were* publicly revealed.

The government's argument also ignores the fact that, in certain (albeit limited) instances, the statute does indeed contemplate disclosure. If a judge finds that "there is no reason to believe that disclosure may endanger the

national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person," he may grant a petition to modify or set aside a nondisclosure order. 50 U.S.C. § 1861(f)(2)(C)(i). Such a petition could presumably only be brought by a § 215 order recipient, because only the recipient, not the target, would know of the order before such disclosure. But this provision indicates that Congress did not expect that all § 215 orders would remain secret indefinitely and that, by providing for such secrecy, Congress did not intend to preclude targets of § 215 orders, should they happen to learn of them, from bringing suit.

(2) Statutory Scheme

The government also relies heavily on Block in arguing that the statutory scheme as a whole impliedly precludes judicial review. In Block, the Supreme Court considered whether consumers of milk could obtain judicial review of milk market orders, which are issued by the Secretary of Agriculture pursuant to the Agricultural Marketing Agreement Act of 1937 ("AMAA"), codified as amended at 7 U.S.C. § 601 et seq. Those orders set the minimum prices that milk processors (also known as "handlers") must pay to milk producers. The Court

held that, in the context of that statute, the statute's silence as to the ability of milk consumers to challenge milk market orders was sufficient to imply that Congress intended that they be precluded from doing so. 467 U.S. at 347. The government would have us view § 215 as a similarly complex administrative scheme that would clearly be disrupted should targets of the orders be permitted judicial review of them.

But the AMAA and the Court's decision in Block are distinguishable from this case. First, the Court in Block, and in its decisions since Block, has made much of whether a statute has administrative review requirements that would be end-run if the APA provided for ordinary judicial review. In Block, for example, the Court noted that, for a milk market order to become effective, the AMAA requires that: (1) the Secretary of Agriculture conduct a rulemaking proceeding before issuing a milk market order; (2) the public be notified of the proceeding and given an opportunity for comment; (3) a public hearing be held, in which (4) the evidence offered shows that the order will further the statute's policy; and (5) certain percentages of milk handlers and producers vote in favor of the orders. See id. at 342.

 428

Such a scheme is a far cry from what is contemplated by § 215. Section 215 contains no administrative review requirements that would be "end run" if targets of the orders were allowed to obtain judicial review thereof. Indeed, the only express mechanism for any review at all of § 215 orders *is* via judicial review – albeit by the FISC, rather than a federal district court.

Unlike the AMAA, § 215 in no way contemplates a "cooperative venture" that precedes the issuance of orders. Id. at 346. In Block, the Court pointed out that the statute provided for milk handlers and producers – and not consumers – to participate in the adoption of the market orders. See id. Those parties, according to the Court, were the ones who could obtain review of the orders, not the consumers, whom Congress had excluded from the entire process. Section 215, in contrast, does not contemplate ex ante cooperation between, for example, telephone companies and the government in deciding how production orders should be crafted and whether they should be approved. To the contrary, under § 215, the government unilaterally crafts orders that may then be approved or not by the FISC. Unlike in the case of the AMAA, there is no indication that Congress, in drafting § 215, intended that the phone companies be the only party

 429

entitled to obtain judicial review of the orders by providing for them to otherwise participate in the order-issuing process.

Block is further distinguishable because the Court there emphasized the fact that "[h]andlers ha[d] interests similar to those of consumers" and could "therefore be expected to challenge unlawful agency action." Id. at 352. Here, in contrast, the interests and incentives of the recipients of § 215 orders are quite different from those of the orders' targets. As appellants point out, telecommunications companies have little incentive to challenge § 215 orders – first, because they are unlikely to want to antagonize the government, and second, because the statute shields them from any liability arising from their compliance with a § 215 order. See 50 U.S.C. § 1861(e). Any interests that they do have are distinct from those of their customers. The telephone service providers' primary interest would be the expense or burden of complying with the orders; only the customers have a direct interest in the privacy of information revealed in their telephone records.

Indeed, courts since Block have interpreted this factor – whether Congress has extended a cause of action to a party whose interests are aligned with those of a party seeking to sue – as critical to the heavily fact-bound Block decision.

The D.C. Circuit has noted that "some discussion in Block . . . sweep[s] broadly" but has concluded that, for example, the AMAA does not preclude milk *producers* (as opposed to *consumers*) from obtaining judicial review of market orders, in part because "[u]nlike the consumers whose interests were coextensive with those of handlers in Block, the producers are the only party with an interest in ensuring that the price paid them is not reduced by too large a[n amount] paid to handlers." Ark. Dairy Coop. Ass'n v. U.S. Dep't of Agric., 573 F.3d 815, 823 (D.C. Cir. 2009) (internal citation omitted). In other words, whether a party with aligned interests can obtain judicial review is an important consideration in interpreting and applying Block.

(3) Legislative History

Finally, the legislative history of the provision for challenging § 215 orders further supports appellants' argument that Congress did not intend to preclude targets of the orders from bringing suit. Appellants point out that the amendment to § 215 that provided for judicial review of § 215 orders in the FISC was passed in response to Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), vacated in part sub nom. Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006). At the same time it added the judicial review provision in § 215, Congress passed a

provision for judicial review in the context of National Security Letters ("NSLs") – a form of administrative subpoenas used to gather communications and records in national security matters. That subsection was added to address the court's concerns in Doe that 18 U.S.C. § 2709, pursuant to which NSLs are issued, "effectively bar[red] or substantially deter[red] any judicial challenge to the propriety of an NSL request." Doe, 334 F. Supp. 2d at 475. Congress's primary purpose in adopting both of these provisions was apparently to clarify that judicial review *was* available to recipients of NSLs and § 215 orders – not to *preclude* review at the behest of the targets of orders. In fact, in Doe, the government argued that the NSL statute already implicitly provided for judicial review. See id. at 492-93. The amendment, therefore, only "clarif[ied] that a FISA 215 order may be challenged and that a recipient of a 215 order may consult with the lawyer and the appropriate people necessary to respond to the order," H.R. Rep. No. 109-174, pt. 1, at 106 (statement of Chairman Sensenbrenner) – both concerns raised by the district court in Doe with respect to NSLs. The amendment was a clarification of the judicial review provision that already implicitly existed; in thus clarifying, it did not affirmatively take away a right to judicial review from another category of individuals not mentioned in the statute.

 432

The government argues that Congress "specifically considered, and rejected, an amendment that would have allowed Section 215 orders to be challenged not only in the FISC, but also in district court." Appellees' Br. 29. But that is an oversimplification of the sequence of events relating to an amendment proposed by Representative Nadler. First, the proposed amendment encompassed more than the issue of judicial review. The amendment primarily proposed a more rigorous standard for obtaining orders under § 215 than existed at the time, and the bulk of the debate on the amendment concerned what degree of suspicion should be required for issuance of a § 215 order. See H.R. Rep. No. 109-174, pt. 1, at 128-32, 135 (2005). Second, the amendment proposed judicial review in a district court by the *recipients* of § 215 orders – a category of persons already granted an avenue of review under § 215, through the FISC process. Id. at 128, 134. It did not address – again, presumably because Congress did not have reason to consider the question at that point – whether a person whose records were seized as a result of such an order would be able, upon learning of the order, to challenge it in district court. Indeed, Representative Nadler specifically noted that his amendment did not grant judicial review at the behest of the "target" of a § 215 order because such a target "doesn't know about" the

order. See id. at 128 (statement of Rep. Nadler) ("It doesn't give the target of the order the ability to go to court. He doesn't know about it."); id. at 134 (statement of Rep. Nadler) ("[T]he fact is that . . . the target of the investigation never hears about this.").

As Justice Scalia has reminded us, moreover, we should exercise caution in relying on this type of legislative history in attempting to discern Congress's intent, because it is so often "impossible to discern what the Members of Congress intended except to the extent that intent is manifested in the *only* remnant of 'history' that bears the unanimous endorsement of the majority in each House: the text of the enrolled bill that became law." Graham County Soil & Water Conservation Dist. v. United States ex rel. Wilson, 559 U.S. 280, 302 (2010) (Scalia, J., concurring) (emphasis in original). Congress's rejection of the Nadler amendment cannot reliably be interpreted as a specific rejection of the opportunity for a § 215 target to obtain judicial review, under the APA or otherwise.

Finally, the government argues that Congress must have intended to preclude judicial review of § 215 orders, because if any customer of a company that receives a § 215 order may challenge such an order, lawsuits could be filed

by a vast number of potential plaintiffs, thus "severely disrupt[ing] . . . the sensitive field of intelligence gathering for counter-terrorism efforts." Appellees' Br. 30 (internal quotation marks omitted).

That argument, however, depends on the government's argument on the merits that bulk metadata collection was contemplated by Congress and authorized by § 215. The risk of massive numbers of lawsuits challenging the same orders, and thus risking inconsistent outcomes and confusion about the legality of the program, occurs only in connection with the existence of orders authorizing the collection of data from millions of people. Orders targeting limited numbers of persons under investigation could be challenged only by the individuals targeted – who, it was expected, would never learn of the orders in the first place. It is only in connection with the government's expansive *use* of § 215 (which, as will be seen below, was not contemplated by Congress) that these risks would create concern.

In any event, restricting judicial review of the legality of § 215 orders under the statute itself would do little to eliminate the specter of duplicative lawsuits challenging orders like the one at issue here. The government does not contend that those whose records are collected pursuant to § 215, assuming they have

established standing, are somehow precluded from bringing constitutional challenges to those orders. The government would thus attribute to Congress a preclusion of statutory challenges that would not eliminate the supposed dangers of multiplicative lawsuits, while channeling those lawsuits toward constitutional issues.

Such an outcome would be anomalous. It would fly in the face of the doctrine of constitutional avoidance, which "allows courts to *avoid* the decision of constitutional questions" by providing "a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." Clark v. Martinez, 543 U.S. 371, 381 (2005) (emphasis in original). In contrast, the approach proffered by the government would preclude lawsuits challenging the legality of § 215 on statutory grounds, while leaving open the path to review of § 215 under the Constitution. While constitutional avoidance is a judicial doctrine, the principle should have considerable appeal to Congress: it would seem odd that Congress would preclude challenges to executive actions that allegedly violate Congress's own commands, and thereby channel the complaints of those aggrieved by such actions into constitutional

challenges that threaten Congress's own authority. There may be arguments in favor of such an unlikely scheme, but it cannot be said that any such reasons are so patent and indisputable that Congress can be assumed, in the face of the strong presumption in favor of APA review, to have adopted them without having said a word about them.

B. Section 2712 and Implied Preclusion

The other potentially relevant exception to the APA's waiver of sovereign immunity looks to whether "any *other* statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702 (emphasis added). The government urges that 18 U.S.C. § 2712, passed in the same statute that contained § 215, is just such a statute, granting as it does a private right of action for money damages against the United States for violations of the Wiretap Act, the Stored Communications Act, and three particular FISA provisions that concern electronic surveillance, physical searches, and pen registers or trap and trace devices (but not § 215). See 18 U.S.C. § 2712(a); see also 50 U.S.C. §§ 1806(a), 1825(a), 1845(a). Section 2712 withdrew the general right to sue the United States under the Wiretap Act and the Stored Communications Act at the same time it added a right of action for money damages. Importantly, it also stated that

 437

"[a]ny action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section." 18 U.S.C. § 2712(d). According to the government, such provisions demonstrate that, where Congress did intend to allow a private right of action for violations of FISA, it did so expressly.

That the provision extending a right of action makes no mention of § 215, however, supports appellants' argument, not the government's. To be sure, "[w]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy . . . to be exclusive, that is the end of the matter; the APA does not undo the judgment." Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak, 132 S. Ct. 2199, 2205 (2012) (second alteration in original) (internal quotation marks omitted). But § 2712 does not deal "in particularity" with § 215. Instead, the government would have us conclude "that in authorizing one person to bring one kind of suit seeking one form of relief, Congress barred another person from bringing another kind of suit seeking another form of relief." Id. at 2209. Section 2712 makes no mention whatsoever of claims under § 215, either to permit them or to preclude them, and, as the Supreme Court stated in Patchak, "[w]e have never held, and see no cause to

hold here, that some general similarity of subject matter can alone trigger a remedial statute's preclusive effect." Id. The "exclusive remedy" provision applies only to claims within the purview of the remedial section, which does not cover all of FISA but rather specifies those FISA provisions to which it applies. Had Congress intended § 2712's exclusive right of action (and its preclusion of other remedies) to extend to § 215, it is fair to assume that it would have also enumerated that section – particularly considering the fact that both provisions were passed in the same statute.

Section 2712, moreover, *explicitly* withdraws the right to challenge the specific government actions taken under specific authorization, in connection with *extending* an explicit cause of action for monetary damages in connection with such actions. First, § 2712 shows that the Congress that enacted the PATRIOT Act understood very well how to withdraw the right to sue under the APA, and to create an exclusive remedy, when it wished to do so. Second, § 2712 manifestly does not create a cause of action for damages for violations of § 215, as it does with respect to those statutes of which it does preclude review under the APA.

Section 2712, therefore, does not preclude appellants' suit here. Nor do the two statutes, when viewed in combination, evince an intent of Congress to preclude suits by targets of § 215 orders.

C. Summary

In short, the government relies on bits and shards of inapplicable statutes, inconclusive legislative history, and inferences from silence in an effort to find an implied revocation of the APA's authorization of challenges to government actions. That is not enough to overcome the strong presumption of the general command of the APA against such implied preclusion. Congress, of course, has the ability to limit the remedies available under the APA; it has only to say so. But it has said no such thing here. We should be cautious in inferring legislative action from legislative inaction, or inferring a Congressional command from Congressional silence. At most, the evidence cited by the government suggests that Congress assumed, in light of the expectation of secrecy, that persons whose information was targeted by a § 215 order would rarely even know of such orders, and therefore that judicial review at the behest of such persons was a non-issue. But such an assumption is a far cry from an unexpressed intention to

 440

withdraw rights granted in a generally applicable, explicit statute such as the APA.

Accordingly, we disagree with the district court insofar as it held that appellants here are precluded from bringing suit against the government, and hold that appellants have a right of action under the APA. We therefore proceed to the merits of the case.

III. Statutory Authorization

Although appellants vigorously argue that the telephone metadata program violates their rights under the Fourth Amendment to the Constitution, and therefore cannot be authorized by either the Executive or the Legislative Branch of government, or by both acting together, their initial argument is that the program simply has not been authorized by the legislation on which the government relies for the issuance of the orders to service providers to collect and turn over the metadata at issue. We naturally turn first to that argument.

Section 215 clearly sweeps broadly in an effort to provide the government with essential tools to investigate and forestall acts of terrorism. The statute permits the government to apply for "an order requiring the production of *any tangible things* . . . for an investigation . . . to protect against international

 441

terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(a)(1) (emphasis added). A § 215 order may require the production of anything that "can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation" or any other court order. Id. § 1861(c)(2)(D).

While the *types* of "tangible things" subject to such an order would appear essentially unlimited, such "things" may only be produced upon a specified factual showing by the government. To obtain a § 215 order, the government must provide the FISC with "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted [under guidelines approved by the Attorney General]." Id. § 1861(b)(2)(A); see id. § 1861(a)(2) (requiring that investigations making use of such orders be conducted under guidelines approved by the Attorney General). The basic requirements for metadata collection under § 215, then, are simply that the records be *relevant* to an *authorized investigation* (other than a threat assessment).

For all the complexity of the statutory framework, the parties' respective positions are relatively simple and straightforward. The government emphasizes that "relevance" is an extremely generous standard, particularly in the context of

 442

the grand jury investigations to which the statute analogizes orders under § 215. Appellants argue that relevance is not an unlimited concept, and that the government's own use (or non-use) of the records obtained demonstrates that most of the records sought are not relevant to any particular investigation; the government does not seek the records, as is usual in a grand jury investigation, so as to review them in search of evidence bearing on a particular subject, but rather seeks the records to create a vast data bank, to be kept in reserve and queried if and when some particular set of records might be relevant to a particular investigation.

Echoing the district court's statement that "'[r]elevance' has a broad legal meaning," 959 F. Supp. 2d at 746, the government argues that the telephone metadata program comfortably meets the requisite standard. The government likens the relevance standard intended by Congress to the standard of relevance for grand jury and administrative subpoenas, and, to some extent, for civil discovery.

Both the language of the statute and the legislative history support the grand jury analogy. During the 2006 reauthorization debate, Senator Kyl recalled that, in passing the PATRIOT Act shortly after September 11, Congress had

realized that "it was time to apply to terrorism many of the same kinds of techniques in law enforcement authorities that we already deemed very useful in investigating other kinds of crimes. Our idea was, if it is good enough to investigate money laundering or drug dealing, for example, we sure ought to use those same kinds of techniques to fight terrorists." 152 Cong. Rec. S1607 (daily ed. Mar. 2, 2006) (statement of Sen. Kyl). He also remarked that "[r]elevance is a simple and well established standard of law. Indeed, it is the standard for obtaining every other kind of subpoena, including administrative subpoenas, grand jury subpoenas, and civil discovery orders." Id. at S1606. And it is well established that "where Congress borrows terms of art . . . , it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken and the meaning its use will convey to the judicial mind unless otherwise instructed." Morissette v. United States, 342 U.S. 246, 250 (1952).

So much, indeed, seems to us unexceptionable. In adopting § 215, Congress intended to give the government, on the approval of the FISC, broad-ranging investigative powers analogous to those traditionally used in connection with grand jury investigations into possible criminal behavior.

The government then points out that, under the accepted standard of relevance in the context of grand jury subpoenas, "courts have authorized discovery of large volumes of information where the requester seeks to identify within that volume smaller amounts of information that could directly bear on the matter." Appellees' Br. 31. The government asks us to conclude that it is "eminently reasonable to believe that Section 215 bulk telephony metadata is relevant to counterterrorism investigations." Id. at 32. Appellants, however, dispute that metadata from every phone call with a party in the United States, over a period of years and years, can be considered "relevant to an authorized investigation," by any definition of the term.

The very terms in which this litigation has been conducted by both sides suggest that the matter is not as routine as the government's argument suggests. Normally, the question of whether records demanded by a subpoena or other court order are "relevant" to a proceeding is raised in the context of a motion to quash a subpoena. The grand jury undertakes to investigate a particular subject matter to determine whether there is probable cause to believe crimes have been committed, and seeks by subpoena records that might contain evidence that will

help in making that determination.[4] Given the wide investigative scope of a grand jury, the standard is easy to meet, but the determination of relevance is constrained by the subject of the investigation. In resolving a motion to quash, a court compares the records demanded by the particular subpoena with the subject matter of the investigation, however broadly defined.

Here, however, the parties have not undertaken to debate whether the records required by the orders in question are relevant to any particular inquiry. The records demanded are all-encompassing; the government does not even suggest that all of the records sought, or even necessarily any of them, are relevant to any specific defined inquiry. Rather, the parties ask the Court to decide whether § 215 authorizes the "creation of a historical repository of information that bulk aggregation of the metadata allows," Appellees' Br. 32, because bulk collection to create such a repository is "necessary to the application

---

[4] Although subpoenas may be used in aid of other court proceedings, we take the grand jury as our example because the powers of the grand jury are particularly wide-ranging, and the standard of relevance or materiality of information sought is much more relaxed than, for example, in a trial, where to be relevant evidence must tend to make a fact "of consequence in determining the action," Fed. R. Evid. 401(b), "more or less probable than it would be without the evidence," id. 401(a).

of certain analytic techniques," Appellants' Br. 23. That is not the language in which grand jury subpoenas are traditionally discussed.

Thus, the government takes the position that the metadata collected – a vast amount of which does not contain directly "relevant" information, as the government concedes – are nevertheless "relevant" because they may allow the NSA, at some unknown time in the future, utilizing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that *is* relevant.[5] We agree with appellants that such an expansive concept of "relevance" is unprecedented and unwarranted.

The statutes to which the government points have never been interpreted to authorize anything approaching the breadth of the sweeping surveillance at issue here.[6] The government admitted below that the case law in analogous

---

[5] Section 215 lists three factors that would render a tangible thing sought "presumptively relevant" to an authorized investigation, see 50 U.S.C. § 1861(b)(2)(A), but the records of ordinary telephone company customers' phone calls do not fall within any of those descriptions.

[6] A recently disclosed, now discontinued program under which the Drug Enforcement Administration utilized administrative subpoenas obtained pursuant to 21 U.S.C. § 876 to collect and maintain a telephone metadata database may have demanded an interpretation approaching the breadth of the government's interpretation of similar language here. See ECF No. 159 (Appellants' Fed. R. App. P. 28(j) letter); ECF No. 161 (Appellees' Fed. R. App. P.

contexts "d[id] not involve data acquisition on the scale of the telephony metadata collection." ACLU v. Clapper, No. 13 Civ. 3994 (S.D.N.Y. Aug. 26, 2013), ECF No. 33 (Mem. of Law of Defs. in Supp. of Mot. to Dismiss) at 24. That concession is well taken. As noted above, if the orders challenged by appellants do not require the collection of metadata regarding every telephone call made or received in the United States (a point asserted by appellants and at least nominally contested by the government), they appear to come very close to doing so. The sheer volume of information sought is staggering; while search warrants and subpoenas for business records may encompass large volumes of paper documents or electronic data, the most expansive of such evidentiary demands are dwarfed by the volume of records obtained pursuant to the orders in question here.

Moreover, the distinction is not merely one of quantity – however vast the quantitative difference – but also of quality. Search warrants and document subpoenas typically seek the records of a particular individual or corporation

---

28(j) letter). That program, which, according to both parties, has been discontinued, is not being challenged here, and we therefore need not opine as to whether the language of the statute pursuant to which the metadata were collected authorized that program.

under investigation, and cover particular time periods when the events under investigation occurred. The orders at issue here contain no such limits. The metadata concerning *every* telephone call made or received in the United States using the services of the recipient service provider are demanded, for an indefinite period extending into the future. The records demanded are not those of suspects under investigation, or of people or businesses that have contact with such subjects, or of people or businesses that have contact with others who are in contact with the subjects – they extend to every record that exists, and indeed to records that do not *yet* exist, as they impose a continuing obligation on the recipient of the subpoena to provide such records on an ongoing basis as they are created. The government can point to no grand jury subpoena that is remotely comparable to the real-time data collection undertaken under this program.

Nevertheless, the government emphasizes the permissive standards applied to subpoenas, noting that, at least in the context of grand jury subpoenas, motions to quash on relevancy grounds are "denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." United States v. R. Enters., Inc., 498 U.S. 292, 301

(1991). That is because such subpoenas "are customarily employed to gather information and make it available to the investigative team of agents and prosecutors so that it can be digested and sifted for pertinent matter" and are therefore "often drawn broadly, sweeping up both documents that may prove decisive and documents that turn out not to be." United States v. Triumph Capital Grp., 544 F.3d 149, 168 (2d Cir. 2008).

In that vein, the government points to cases in which courts have upheld subpoenas for broad categories of information and for "large-scale collection[] of information." Appellees' Br. 33 (internal quotation marks omitted). For example, in In re Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d 301 (8th Cir. 1987), the Eighth Circuit denied Western Union's motion to quash a subpoena that requested production by Western Union's primary wire service agent in Kansas City of all money order applications for amounts over $1,000 over a more than two-year period, and of a report summarizing all wire transactions it conducted over an approximate one-year period. Despite Western Union's argument that the subpoena would sweep in "records involving hundreds of innocent people," the court stated that grand juries are not necessarily prohibited from engaging in "dragnet operation[s]." Id. at 305 (internal quotation marks

450

omitted). In In re Subpoena Duces Tecum, 228 F.3d 341 (4th Cir. 2000), the Fourth Circuit also denied a motion to quash a subpoena issued to a doctor requiring production of, inter alia, all patient records and documentation concerning patients whose services were billed to Medicare, Medicaid, and a number of insurance companies, including the patients' complete medical files, their billing records, office appointment books, sign-in sheets, and telephone messages, over a period of at least seven years. That court held that the subpoena did not sweep too broadly, despite the high volume of documents it demanded, in part because of the scope of the fraud being investigated and the size of the doctor's practice. Id. at 350-51; see also Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946) ("[R]elevancy and adequacy or excess in the breadth of the subpoena are matters variable in relation to the nature, purposes and scope of the inquiry.").

But broad as those subpoenas were, the cases cited by the government only highlight the difference between the investigative demands at issue in those cases and the ones at issue here. Both of those examples, and all examples of which we are aware, are bounded either by the facts of the investigation or by a finite time limitation. The telephone metadata program requires that the phone companies

turn over records on an "ongoing daily basis" – with no foreseeable end point, no requirement of relevance to any particular set of facts, and no limitations as to subject matter or individuals covered.[7] Even in the Eighth Circuit case that the government cites, moreover, although it upheld the subpoena at issue, the Eighth Circuit suggested that the district court "consider the extent to which the government would be able to identify in advance . . . patterns or characteristics that would raise suspicion . . . designed to focus on illegal activity without taking in an unnecessary amount of irrelevant material." In re Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d at 305-06. Courts have typically looked to constrain even grand jury subpoenas to a standard of reasonableness related to a defined investigative scope; we have found excessively broad a subpoena requiring production of all of an accountant's files within a mere three filing

[7] Drawing an analogy again to the context of administrative subpoenas, we note too that courts are "more reluctant to enforce subpoenas when agencies have sought records of third parties who were not targets of the agency's investigation." In re McVane, 44 F.3d 1127, 1137 (2d Cir. 1995). The overwhelming bulk of the metadata collected by the telephone metadata program, as the government itself concedes, concerns "third parties" in that sense of the word – individuals who are not targets of an investigation or suspected of engaging in any crime whatsoever, and who are not even suspected of having any contacts with any such targets or suspects. Their records are sought solely to build a repository for the future application of the investigative techniques upon which the program relies.

cabinets, "without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period," because it swept in papers that there was no reason to believe were relevant. In re Horowitz, 482 F.2d 72, 79 (2d Cir. 1973). We therefore limited the subpoena's time period absent the government's making a minimal showing of relevance. Id. at 79-80.

To the extent that § 215 was intended to give the government, as Senator Kyl proposed, the "same kinds of techniques to fight terrorists" that it has available to fight ordinary crimes such as "money laundering or drug dealing," 152 Cong. Rec. S1607 (daily ed. Mar. 2, 2006) (statement of Sen. Kyl), the analogy is not helpful to the government's position here. The techniques traditionally used to combat such ordinary crimes have not included the collection, via grand jury subpoena, of a vast trove of records of metadata concerning the financial transactions or telephone calls of ordinary Americans to be held in reserve in a data bank, to be searched if and when at some hypothetical future time the records might become relevant to a criminal investigation.

The government's emphasis on the potential breadth of the term "relevant," moreover, ignores other portions of the text of § 215. "Relevance"

does not exist in the abstract; something is "relevant" or not in relation to a particular subject. Thus, an item relevant to a grand jury investigation may not be relevant at trial. In keeping with this usage, § 215 does not permit an investigative demand for any information relevant to fighting the war on terror, or anything relevant to whatever the government might want to know. It permits demands for documents "relevant to an authorized *investigation*." The government has not attempted to identify to what particular "authorized investigation" the bulk metadata of virtually all Americans' phone calls are relevant. Throughout its briefing, the government refers to the records collected under the telephone metadata program as relevant to "counterterrorism investigations," without identifying any specific investigations to which such bulk collection is relevant. See, e.g., Appellees' Br. 32, 33, 34.[8] The FISC orders, too, refer only to "authorized investigations (other than threat assessments) being

[8] While the government purports to have provided "examples" of "specific counter-terrorism investigations," see Appellees' Br. 33, citing Joint App'x 254-55, those examples serve only as instances in which the metadata already collected in bulk were able to be queried and resulted in identification of a previously unknown contact of known terrorists. The government does not contend that most of the metadata already collected were relevant to any of those particular investigations, let alone that it was able to so demonstrate prior to the collection of those metadata.

conducted by the FBI . . . to protect against international terrorism," see, e.g., 2006 Primary Order at 2; Joint App'x 127, 317, merely echoing the language of the statute. The PCLOB report explains that the government's practice is to list in § 215 applications multiple terrorist organizations, and to declare that the records being sought are relevant to the investigations of all of those groups. PCLOB Report 59. As the report puts it, that practice is "little different, in practical terms, from simply declaring that they are relevant to counterterrorism in general. . . . At its core, the approach boils down to the proposition that essentially all telephone records are relevant to essentially all international terrorism investigations." Id. at 59-60. Put another way, the government effectively argues that there is only one enormous "anti-terrorism" investigation, and that any records that might ever be of use in developing any aspect of that investigation are relevant to the overall counterterrorism effort.

The government's approach essentially reads the "authorized investigation" language out of the statute. Indeed, the government's information-gathering under the telephone metadata program is inconsistent with the very concept of an "investigation." To "investigate" something, according to the Oxford English Dictionary, is "[t]o search or inquire into; to

examine (a matter) systematically or in detail; to make an inquiry or examination into."[9] 8 Oxford English Dictionary 47 (2d ed. 2001). Section 215's language thus contemplates the specificity of a particular investigation – not the general counterterrorism intelligence efforts of the United States government. But the records in question here are not sought, at least in the first instance, because the government plans to examine them in connection with a "systematic examination" of anything at all; the records are simply stored and kept in reserve until such time as some particular investigation, in the sense in which that word is traditionally used in connection with legislative, administrative, or criminal inquiries, is undertaken. Only at that point are any of the stored records examined. The records sought are not even asserted to be relevant to any on-going "systematic examination" of any particular suspect, incident, or group; they are relevant, in the government's view, because there might at some future point be a need or desire to search them in connection with a hypothetical future inquiry.

---

[9] The noun form "investigation" is similarly defined as "[t]he action of investigating; the making of a search or inquiry; systematic examination; careful and minute research." 8 Oxford English Dictionary 47 (2d ed. 2001).

The government's approach also reads out of the statute another important textual limitation on its power under § 215. Section 215 permits an order to produce records to issue when the government shows that the records are "relevant to an authorized investigation *(other than a threat assessment)*." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). The legislative history tells us little or nothing about the meaning of "threat assessment." The Attorney General's Guidelines for Domestic FBI Operations, however, tell us somewhat more. The Guidelines divide the category of "investigations and intelligence gathering" into three subclasses: assessments, predicated investigations (both preliminary and full), and enterprise investigations. See Attorney General's Guidelines for Domestic FBI Operations 16-18 (2008), https://www.ignet.gov/sites/default/files/files/invprg1211appg1.pdf. Assessments are distinguished from investigations in that they may be initiated without any factual predication. Id. at 17. The Guidelines cite the objective of preventing the commission of terrorist acts against the nation as an example of a proper assessment objective, stating that the FBI "must proactively draw on available sources of information to identify terrorist threats and activities." Id. The methods used in assessments are "generally those of relatively low-

intrusiveness, such as obtaining publicly available information, checking government records, and requesting information from members of the public." Id. at 17-18. Because of that low level of intrusiveness, the Guidelines do not require supervisory approval for assessments, although FBI policy may require it in particular cases, depending on the assessment's purpose and the methods being used. Id. at 18.

The FBI Domestic Investigations and Operations Guide elaborates on this scheme. It too provides that threat assessments "do not require a particular factual predication but do require an authorized purpose and clearly defined objective(s). Assessments may be carried out to detect, obtain information about, or prevent or protect against Federal crimes or threats to the national security or to collect foreign intelligence." FBI Domestic Investigations and Operations Guide § 5.1 (2011), http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version/fbi-domestic-investigations-and-operations-guide-diog-october-15-2011-part-01-of-03/view. Although no specific factual predicate is required, the

Guide makes clear that assessments cannot be based on "arbitrary or groundless speculation." Id. It adds:

> Although difficult to define, "no particular factual predication" is less than "information or allegation" as required for the initiation of a preliminary investigation (PI). .For example, an Assessment may be conducted when: (i) there is reason to collect information or facts to determine whether there is a criminal or national security threat; and (ii) there is a rational and articulable relationship between the stated authorized purpose of the Assessment on the one hand and the information sought and the proposed means to obtain that information on the other.

Id.

In limiting the use of § 215 to "investigations" rather than "threat assessments," then, Congress clearly meant to *prevent* § 215 orders from being issued where the FBI, without any particular, defined information that would permit the initiation of even a preliminary investigation, sought to conduct an inquiry in order to identify a potential threat in advance. The telephone metadata program, however, and the orders sought in furtherance of it, are even more remote from a concrete investigation than the threat assessments that – however important they undoubtedly are in maintaining an alertness to possible threats to national security – Congress found not to warrant the use of § 215

orders. After all, when conducting a threat assessment, FBI agents must have both a reason to conduct the inquiry and an articulable connection between the particular inquiry being made and the information being sought. The telephone metadata program, by contrast, seeks to compile data in advance of the need to conduct any inquiry (or even to examine the data), and is based on no evidence of any current connection between the data being sought and any existing inquiry.

We agree with the PCLOB, which concluded that the government's rationale for the "relevance" of the bulk collection of telephone metadata "undermines" the prohibition on using § 215 orders for threat assessments:

> [Section 215] provides that records cannot be obtained for a "threat assessment," meaning those FBI investigatory activities that "do not require a particular factual predicate." By excluding threat assessments from the types of investigations that can justify an order, Congress directed that Section 215 not be used to facilitate the broad and comparatively untethered investigatory probing that is characteristic of such assessments. But by collecting the nation's calling records *en masse*, under an expansive theory of their relevance to multiple investigations, the NSA's program undercuts one of the functions of the "threat assessment" exclusion: ensuring that records are not acquired by the government without some reason to suspect a connection between those records and a specific, predicated terrorism investigation. While the rules

460

> governing the program limit the *use* of telephone records to searches that are prompted by a specific investigation, the relevance requirement in Section 215 restricts the *acquisition* of records by the government.

PCLOB Report 60 (emphases in original) (footnote omitted).[10]

The interpretation urged by the government would require a drastic expansion of the term "relevance," not only with respect to § 215, but also as that term is construed for purposes of subpoenas, and of a number of national security-related statutes, to sweep further than those statutes have ever been thought to reach. For example, the same language is used in 18 U.S.C. § 2709(b)(1) and 20 U.S.C. § 1232g(j)(1)(A), which authorize, respectively, the compelled production of telephone toll-billing and educational records relevant to authorized investigations related to terrorism. There is no

[10] The government also argues that, aside from their relevance to the subject matter of counterterrorism, the telephone metadata records are relevant to authorized investigations in that they are necessary for the government to apply certain investigative techniques – here, searching based on "selectors" through the government's metadata repository. That argument proves too much. If information can be deemed relevant solely because of its necessity to a particular process that the government has chosen to employ, regardless of its subject matter, then so long as "the government develops an effective means of searching through *everything* in order to find *something*, . . . *everything* becomes relevant to its investigations" – and the government's "technological capacity to ingest information and sift through it efficiently" would be the only limit to what is relevant. PCLOB Report 62 (emphases in original).

evidence that Congress intended for those statutes to authorize the bulk collection of every American's toll-billing or educational records and to aggregate them into a database — yet it used nearly identical language in drafting them to that used in § 215. The interpretation that the government asks us to adopt defies any limiting principle. The same rationale that it proffers for the "relevance" of telephone metadata cannot be cabined to such data, and applies equally well to other sets of records. If the government is correct, it could use § 215 to collect and store in bulk any other existing metadata available anywhere in the private sector, including metadata associated with financial records, medical records, and electronic communications (including e-mail and social media information) relating to all Americans.

Such expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans. Perhaps such a contraction is required by national security needs in the face of the dangers of contemporary domestic and international terrorism. But we would expect such a momentous decision to be preceded by substantial debate, and expressed in unmistakable language. There is no evidence of such a debate in the legislative history of § 215, and the

language of the statute, on its face, is not naturally read as permitting investigative agencies, on the approval of the FISC, to do any more than obtain the sorts of information routinely acquired in the course of criminal investigations of "money laundering [and] drug dealing."

We conclude that to allow the government to collect phone records only because they may become relevant to a possible authorized investigation in the future fails even the permissive "relevance" test. Just as "the grand jury's subpoena power is not unlimited," United States v. Calandra, 414 U.S. 338, 346 (1974), § 215's power cannot be interpreted in a way that defies any meaningful limit. Put another way, we agree with appellants that the government's argument is "irreconcilable with the statute's plain text." Appellants' Br. 26. Such a monumental shift in our approach to combating terrorism requires a clearer signal from Congress than a recycling of oft-used language long held in similar contexts to mean something far narrower. "Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions — it does not . . . hide elephants in mouseholes." Whitman v. Am. Trucking Ass'ns., 531 U.S. 457, 468 (2001). The language of § 215 is decidedly too ordinary for what the government would have us believe is such an

extraordinary departure from any accepted understanding of the term "relevant to an authorized investigation."

Finally, as it did with respect to the question of judicial review, the government again resorts to the claim that if Congress did not *explicitly* adopt the rule for which it argues, it did so *implicitly*. Here, the government argues that Congress has ratified the FISC's interpretation of § 215, and thus the telephone metadata program, by reauthorizing § 215 in 2010 and 2011. We reject that argument.

First, the theory of congressional ratification of judicial interpretations of a statute by reenactment cannot overcome the plain meaning of a statute. "Where the law is plain, subsequent reenactment does not constitute an adoption of a previous administrative construction." Demarest v. Manspeaker, 498 U.S. 184, 603 (1991).

Second, although "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change," Lorillard v. Pons, 434 U.S. 575, 580 (1978), there are limits to that presumption — particularly where, as here, knowledge of the program was intentionally kept to a minimum, both within Congress and among

the public. We have said that, at least in the case of an administrative interpretation of a statute, for the doctrine of legislative ratification to apply, we must first "ascertain whether Congress has spoken clearly enough to constitute acceptance and approval of an administrative interpretation. Mere reenactment is insufficient." Isaacs v. Bowen, 865 F.2d 468, 473 (2d Cir. 1989). In Atkins v. Parker, the Supreme Court applied the doctrine of legislative ratification where "Congress was . . . well aware of, and legislated on the basis of, . . . contemporaneous administrative practice," concluding that it therefore "must be presumed to have intended to maintain that practice absent some clear indication to the contrary." 472 U.S. 115, 140 (1985). In contrast, in a situation in which "there [wa]s nothing to indicate that [the interpretation of a regulation] was ever called to the attention of Congress," and the statute's reenactment "was not accompanied by any congressional discussion which throws light on its intended scope," the Court has "consider[ed] the . . . re-enactment to be without significance." United States v. Calamaro, 354 U.S. 351, 359 (1957); see also Comm'r v. Glenshaw Glass Co., 348 U.S. 426, 431 (1955) ("Re-enactment [of a statute] – particularly without the slightest affirmative indication that Congress ever had [a particular] decision before it – is an unreliable indicium at best.").

Third, as the above precedents suggest, the public nature of an interpretation plays an important role in applying the doctrine of legislative ratification. The Supreme Court has stated that "[w]here an agency's statutory construction has been fully brought to the attention of the public and the Congress, and the latter has not sought to alter that interpretation although it has amended the statute in other respects, then presumably the legislative intent has been correctly discerned." North Haven Bd. of Educ. v. Bell, 456 U.S. 512, 535 (1982) (internal quotation marks omitted); see also United States v. Chestman, 947 F.2d 551, 560 (2d Cir. 1991). Congressional inaction is already a tenuous basis upon which to infer much at all, even where a court's or agency's interpretation is fully accessible to the public and to all members of Congress, who can discuss and debate the matter among themselves and with their constituents. But here, far from the ordinarily publicly accessible judicial or administrative opinions that the presumption contemplates, no FISC opinions authorizing the program were made public prior to 2013 — well after the two occasions of reauthorization upon which the government relies, and despite the fact that the FISC first authorized the program in 2006.

Congress cannot reasonably be said to have ratified a program of which many members of Congress – and all members of the public – were not aware. In 2010, the Senate and House Intelligence Committees requested that the Executive Branch provide all members of Congress access to information about the program before the reauthorization vote. In response, the Executive Branch provided the Intelligence Committee chairs with a classified paper on the program, which was then made available to members of Congress. That availability, however, was limited in a number of ways. First, the briefing papers could only be viewed in secure locations, for a limited time period and under a number of restrictions. See Joint App'x 148-165. The government does not dispute appellants' assertion that members of Congress could not bring staff with them when they went to read the briefing papers, nor discuss the program with their staff. And, of course, no public debate on the program took place. In 2011, briefing papers were also provided to the Intelligence Committees, but only the Senate Committee shared the papers with other members of that body who were not committee members. The House Intelligence Committee did not share the papers at all with non-members, leaving the non-committee Representatives in

the dark as to the program. See generally id. at 170-73; see also Clapper, 959 F. Supp. 2d at 745.

To be sure, the government is correct that whether a particular interpretation was legislatively ratified ordinarily should not depend on the "number of legislators with actual knowledge of the government's interpretation." Appellees' Br. 36. We do not insist, in the ordinary case, on evidence that members of Congress actually read and understood administrative or judicial decisions interpreting a statute to apply the doctrine of ratification. But this is far from the ordinary case. In the ordinary case in which we apply the Lorillard presumption, the administrative or judicial interpretation argued to have been ratified by Congress was available to the public in published sources. Concerned citizens and interest groups had every opportunity to bring interpretations that they believed were incorrect or undesirable to the attention of their representatives in the House and Senate, and to lobby for legislation rejecting those interpretations. To the extent that some members of Congress were unaware of the details of those interpretations, their ignorance itself very likely reflected the absence of any particular controversy surrounding them.

In sharp contrast, the telephone metadata program was (for understandable reasons) shrouded in the secrecy applicable to classified information, and only a limited subset of members of Congress had a comprehensive understanding of the program or of its purported legal bases. There was certainly no opportunity for broad discussion in the Congress or among the public of whether the FISC's interpretation of § 215 was correct.[11] Finding the government's interpretation of the statute to have been "legislatively ratified" under these circumstances would ignore reality. Practically speaking, it is a far stretch to say that Congress was aware of the FISC's legal interpretation of § 215 when it reauthorized the statute in 2010 and 2011. We therefore cannot accept the argument that Congress, by reauthorizing § 215 without change in 2010 and 2011, thereby legislatively ratified the interpretation of § 215 urged by the government. The widespread controversy that developed, in and out of Congress, upon the public disclosure of the program makes clear that this is not a

[11] Indeed, the discrepancy between the conclusion we reach herein and that reached by the FISC may, at least in part, be accounted for by our having received the benefit of an adversarial presentation of the issues. See post at pp. 6, 11 (Sack, J., concurring).

situation in which Congress quietly but knowingly adopted the FISC's interpretation of § 215 because there was no real opposition to that interpretation.

For all of the above reasons, we hold that the text of § 215 cannot bear the weight the government asks us to assign to it, and that it does not authorize the telephone metadata program. We do so comfortably in the full understanding that if Congress chooses to authorize such a far-reaching and unprecedented program, it has every opportunity to do so, and to do so unambiguously. Until such time as it does so, however, we decline to deviate from widely accepted interpretations of well-established legal standards. We therefore disagree with the district court insofar as it held that appellants' statutory claims failed on the merits, and vacate its judgment dismissing the complaint.

IV. Constitutional Claims

In addition to arguing that the telephone metadata program is not authorized by § 215, appellants argue that, even if the program is authorized by statute, it violates their rights under the Fourth and First Amendments to the

Constitution. The Fourth Amendment claim, in particular, presents potentially vexing issues.[12]

Appellants contend that the seizure from their telephone service providers, and eventual search, of records of the metadata relating to their telephone communications violates their expectations of privacy under the Fourth Amendment in the absence of a search warrant based on probable cause to believe that evidence of criminal conduct will be found in the records. The government responds that the warrant and probable cause requirements of the Fourth Amendment are not implicated because appellants have no privacy rights in the records. This dispute touches an issue on which the Supreme Court's jurisprudence is in some turmoil.

---

[12] For that reason, we discuss infra some of the Fourth Amendment concerns that the program implicates. As to the First Amendment issues, appellants argue that the program infringes their First Amendment associational privacy and free speech rights, "substantially impair[ing]" those rights by "expos[ing] their telephonic associations to government monitoring and scrutiny." Appellants' Br. 53. They contend that the program must therefore survive "exacting scrutiny." Id. at 58. The government responds, as to the merits of appellants' First Amendment claim, that any such burdens are merely "incidental." Appellees' Br. 54. As noted infra, because we find that the telephone metadata program exceeds the bounds of what is authorized by § 215, we need not reach either constitutional issue, and we see no reason to discuss the First Amendment claims in greater depth.

In Katz v. United States, 389 U.S. 347 (1967), the Supreme Court departed from the property-based approach to the Fourth Amendment that had governed since Olmstead v. United States, 277 U.S. 438 (1928), which depended upon whether an actual physical trespass of property had occurred. As explained in Justice Harlan's concurring opinion, the Court held in Katz that a search occurs where "a person ha[s] exhibited an actual (subjective) expectation of privacy, and . . . the expectation [is] one that society is prepared to recognize as 'reasonable.'" 389 U.S. at 361 (Harlan, J., concurring).

The Supreme Court has also long held, however, that individuals have no "legitimate expectation of privacy in information [they] voluntarily turn[] over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979); see, e.g., California v. Greenwood, 486 U.S. 35 (1988) (no objectively reasonable expectation of privacy in garbage exposed to the public by being placed on a sidewalk); United States v. Miller, 425 U.S. 435 (1976) (no legitimate expectation of privacy in bank records). In Smith v. Maryland, the Court applied that doctrine to uphold the constitutionality of installing a pen register at a telephone company's office that recorded the numbers dialed from a criminal suspect's home telephone. 442 U.S. at 737, 745-46. The Court held that the installation of the pen register was not a

search for Fourth Amendment purposes because, by placing calls, individuals expose the telephone numbers they dial to the telephone company and therefore "assume[] the risk that the company [may] reveal to police the numbers . . . dialed." Id. at 744. Similarly, it has long been commonplace for grand juries to subpoena an individual's telephone records from the individual's telephone service provider, in the absence of probable cause or a warrant issued by a judge. The acquisition of such records, it has been held, implicates no legitimate privacy interest of the subscriber, because the records are not his or hers alone. See, e.g., id. at 742-44; Miller, 425 U.S. at 443; Couch v. United States, 409 U.S. 322, 334-36 (1973). The subscriber cannot reasonably believe that the records are private, because he or she has voluntarily exposed the information contained in them to the telephone company, which uses them for its own business purpose of billing the subscriber.

The government argues, and the district court held, that this doctrine requires rejection of appellants' claim that the acquisition of telephone metadata (as opposed to the contents of communications) violates the Fourth Amendment, or even implicates its protections at all. Appellants respond that modern

technology requires revisitation of the underpinnings of the third-party records doctrine as applied to telephone metadata.

Appellants' argument invokes one of the most difficult issues in Fourth Amendment jurisprudence: the extent to which modern technology alters our traditional expectations of privacy. On the one hand, the very notion of an individual's expectation of privacy, considered in Katz a key component of the rights protected by the Fourth Amendment, may seem quaint in a world in which technology makes it possible for individuals and businesses (to say nothing of the government) to observe acts of individuals once regarded as protected from public view. On the other hand, rules that permit the government to obtain records and other information that consumers have shared with businesses without a warrant seem much more threatening as the extent of such information grows.

Appellants point to the Supreme Court's decision in United States v. Jones, 132 S. Ct. 945 (2012), as exemplifying the kind of challenge to apparently established law that they seek to bring. Jones does not address telephone or other business records, but arose in the somewhat analogous context of physical surveillance. Prior to Jones, in United States v. Knotts, 460 U.S. 276 (1983), in a

ruling based in substantial part on the core notion that an individual has no expectation of privacy in what he exposes to the eyes of third parties, the Court held that a person has no expectation of privacy in his public movements, because he "voluntarily convey[s] to anyone who want[s] to look the fact that he [i]s traveling on particular roads in a particular direction, the fact of whatever stops he ma[kes], and the fact of his final destination." Id. at 281-82. The Court therefore ruled that, just as police agents may follow a suspect in public without a warrant or probable cause, the government's use of a beeper to follow a suspect without a warrant was constitutional; the beeper merely "augment[ed]" the officers' normal sensory faculties, but did nothing that an individual otherwise monitoring the suspect could not do without it. Id. at 282. The Court noted, however, in response to concern about the potential for twenty-four hour surveillance without judicial supervision, that "if . . . dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." Id. at 284.

That opportunity came decades later, in Jones. In that case, the government had tracked an individual's location over the course of 28 days using

a GPS tracking device it had attached to his vehicle without first obtaining a warrant. 132 S. Ct. at 948. The D.C. Circuit held that, because an individual does not expose his location to the public over the course of an entire month, either actually or constructively, the proper framework from which to analyze the operation was not a variation on the third-party doctrine but instead Katz's reasonable expectation of privacy standard. United States v. Maynard, 615 F.3d 544, 555-63 (D.C. Cir. 2010), aff'd on other grounds sub nom. Jones, 132 S. Ct. 945. It held that the defendant's expectation of privacy had been violated, because the long-term surveillance revealed a "mosaic" of information in which individuals had privacy interests, even in the absence of a privacy interest in discrete pieces of such information. Id. at 562-63.

The Supreme Court affirmed the D.C. Circuit's opinion, but on different grounds. It held that the operation was a search entitled to Fourth Amendment protection because the attachment of the GPS device constituted a technical trespass on the defendant's vehicle. Jones, 132 S. Ct. at 949-53. The Court's majority opinion declined to reach the issue of whether the operation would have passed Katz's "reasonableness" test, id. at 954, or whether the third-party doctrine instead applied, id. at 952.

As appellants note, however, five of the Justices appeared to suggest that there might be a Fourth Amendment violation even without the technical trespass upon which the majority opinion relied. Four of the Justices argued that the Court should have applied the Katz "reasonableness" test, and that the surveillance would not survive that test. Id. at 957-58, 964 (Alito, J., concurring). Justice Sotomayor noted in another concurring opinion that "the majority opinion's trespassory test may provide little guidance" for certain modern-day surveillance techniques, for which physical trespass is often not necessary. Id. at 955 (Sotomayor, J., concurring). Consequently, she observed that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," noting that such an approach is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." Id. at 957.

Appellants argue that the telephone metadata program provides an archetypal example of the kind of technologically advanced surveillance techniques that, they contend, require a revision of the third-party records doctrine. Metadata today, as applied to individual telephone subscribers,

MADHEWOO M. v THE STATE OF MAURITIUS AND ANOR

2015 SCJ 177

Record No. 108696

IN THE SUPREME COURT OF MAURITIUS

In the matter of:

Maharajah Madhewoo

Plaintiff

v.

1. The State of Mauritius
2. The Minister of Information and Communication Technology

Defendants

JUDGMENT

Introduction: The declaratory orders sought

In the present action entered by way of a plaint with summons the plaintiff seeks from this Court a judgment declaring that –

> *"(1) the implementation of the new biometric identity card as per the National Identity Card Act 2013 by the agents and/or the employees of the Defendants, is in breach of Sections 1, 2, 3, 4, 5, 7, 9, 15, 16, 45 of the spirit of Constitution coupled with Article 22 of the Civil Code and therefore null and void;*
>
> *(2) the blanket power of collection and the indefinite storage of personal biometric data including the finger prints on the biometric identity card of citizens including Plaintiff by the agents and/or the employees of the Defendants are in breach of Sections 1, 2, 3, 4, 5, 7, 9, 15, 16, 45 of the spirit of Constitution coupled with Article 22 of the Civil Code and therefore null and void."*

Preliminary remarks

As a result of general elections which took place after judgment had been reserved in the present case, a new government with new Ministers took over. As the new Minister of

Information and Communication Technology was himself a plaintiff in a similar case before this Bench, the case was fixed for mention in view of ascertaining whether the stand of the

479

defendant No 2 was still the same. Although the statements of Counsel for the defendants were rather evasive, the stand of the defendant No 2 has remained the same both in facts and in law.

The essential undisputed facts:

The following essential facts, as can be gathered from the common statement of agreed facts filed by the parties, are not in dispute:

1. The plaintiff is a citizen of the Republic of Mauritius;

2. The National Identity Card (Miscellaneous Provisions) Bill (No. XVII of 2013) was passed on 9th July 2013;

3. The implementation of the new biometric identity card project, which was widely publicized, started as from 1st October 2013 and all adult citizens of the Republic of Mauritius have since then been under a legal obligation to apply for a new biometric Identity Card to replace the former one.

4. To obtain the new biometric Identity Card, existing card holders must register at an Identity Card Conversion Centre in Mauritius, while persons applying for an identity card for the first time have to register at the National Identity Card Unit of the Civil Status Division;

5. The National Identity Card Act provides that every person applying for an identity card is under an obligation to, *inter alia*:

   (i) allow his fingerprints, and other biometric information about himself to be taken and recorded; and

   (ii) allow himself to be photographed.

6. To get the new Identity Card, Plaintiff will have to provide biometric information, namely his fingerprints and photograph, to employees of the Defendants.

480

7. Plaintiff has, as at date, not applied for a biometric identity card;

8. In a number of articles in newspapers and their online versions, as listed in the parties' common statement of agreed facts, concern and qualms have been expressed about the giving of fingerprints and about other data to be contained in the new identity card.

9. The total cost of implementing the Mauritius National Identity Card Project on a turnkey basis proposed by the Singapore consortium is estimated at Rs 1.1 billion.

Outstanding issues raised in the *plea in limine*

The following points, which were raised in a plea *in limine* at the stage of pleadings, were not pressed prior to evidence being heard, but are now being raised:

(a) that adequate alternative means of redress are open to the plaintiff;
(b) that the plaintiff has failed to disclose the sections of the law under which the application for redress has been made;
(c) that the plaint does not state with precision the provisions of the Constitution which have allegedly been contravened;
(d) that the nature of the relief sought has not been stated with precision;
(e) that the defendant No. 2 should be put out of cause as a defendant as there is no prayer directed against him in that capacity.

We shall now deal with those points:

(a) The contention that adequate means of redress are open to the plaintiff

As regards (a) above, section 17(2) of the Constitution, which provides for the jurisdiction of the Supreme Court to hear applications for redress where a person alleges that any of sections 3 to 16 has been, is being or is likely to be contravened in relation to him, contains the following proviso:

> *"Provided that the Supreme Court shall not exercise its powers under this subsection if it is satisfied that adequate means of redress for the contravention alleged are or have been available to the person concerned under any other law."*

481

It is the defendants' submission that the adequate means of redress for the contravention alleged by the plaintiff are available to the plaintiff under the Data Protection Act. That Act, they point out, provides adequate investigatory and enforcement safeguards against the misuse of personal data.

In our view, this submission is based on incorrect reasoning as the defendants cannot invoke a law the constitutionality of which is put in question as the law under which an alternative means of redress lies.

(b) **The alleged failure to disclose the section of the Constitution under which the application has been made**

In relation to (b) above, we are of the view that it is clear enough from the plaint, what are the sections of the law under which the application has been made. Section 17(1) of the Constitution reads as follows:

> *"Where any person alleges that any of sections 3 to 16 has been, is being or is likely to be contravened in relation to him, then, without prejudice to any other action with respect to the same matter that is lawfully available, that person may apply to the Supreme Court for redress."*

And section 83(1) of the Constitution provides:

> *"Subject to sections 41(5), 64(5) and 101(1), where any person alleges that any provision of this Constitution (other than Chapter II) has been contravened and that his interests are being or are likely to be affected by such contravention, then, without prejudice to any other action with respect to the same matter which is lawfully available, that person may apply to the Supreme Court for a declaration and for relief under this section."*

The alleged breaches of sections 1, 2, 3, 4, 5, 7, 9, 15 and 16 as mentioned in the plaint make it tolerably clear that redress in that connection is being sought under section 17(1) of the Constitution. Similarly, the alleged breach of section 45 falls squarely under the redress provided for in section 83(1), bearing in mind that the subsections 41(5), 64(5) and 101(1) to which the provision in section 83(1) is subjected are not applicable in the present case.

482

(c) **The alleged failure to state with precision in the plaint which provisions of the Constitution have allegedly been contravened**

It is laid down in rule 2(1) of the Supreme Court (Constitutional Relief) Rules 2000 that an application for constitutional relief must state with precision the provision of the Constitution which is said to have been, or to be likely to be, contravened. It is beyond dispute that the provisions of the Constitution which are alleged in the plaint to have been or to be about to be contravened are specified. In our view, there has been sufficient compliance by the plaintiff with rule 2(1) above and the submission of the defendants that the plaintiff has failed "*to state with sufficient precision the way in which the provisions of sections 1, 2, 4, 7, 13, 15 and 45 have been breached*" is not, in our view well grounded.

It is apposite at this juncture to point out, in relation to the points raised at heading (b) and the present heading, that, as conceded by the defendants in their written submissions, this Court has often observed that objections of a procedural nature should not be a bar to the vindication of fundamental human rights.

(d) **The allegation that the nature of the relief sought has not been stated with precision**

Here too is an allegation which is to our minds unwarranted. In the introductory part of this judgment we have set out the declaratory orders sought under the plaint. This is, in our view sufficient compliance with rule 2(1) of the Supreme Court (Constitutional Relief) Rules 2000 which requires the application to state with precision the nature of the relief sought.

In their written submissions, Counsel for the defendants have pointed out that the "National Identity Card Act 2013" as referred to in the first declaratory order sought does not exist. However, nobody can be misled by the incorrect mention of the year 2013 after the correct appellation of the Act – "The National Identity Card Act". Indeed it can be gathered from the agreed statement of facts, the agreed statement of disputed facts and the common statement of outstanding issues of law, that the provision of law the implementation of which is being contested is section 4(2)(c), as amended by section 15 of Act 20 of 2009 to introduce the requirement that every person who applies for an identity card shall "*allow his fingerprints and other biometric information about himself, to be taken and recorded*" for the purpose of the identity card. That amendment came into operation on 16 September 2013 by virtue of Proclamation 42 of 2013, and this is no

doubt the explanation for the erroneous reference to the "*National Identity Card Act 2013*".

(e) **The contention that defendant No. 2 should be put out of cause**

It is contended by the defendant No. 2 that he should be put out of cause as a defendant inasmuch as there is no prayer against him. A perusal of the plaint shows, however, that the declaratory orders sought in paragraph 27 of the plaint with summons are in respect of the implementation of the new biometric card and the collection and indefinite storage of personal biometric data by the agents and employees of both defendants. The defendant No. 2 cannot in the circumstances be put out of cause.

In view of our conclusions above, all the outstanding points contained in the plea *in limine* and raised at the end of the trial, must fail.

The alleged breaches of the Constitution

We now turn to the alleged breaches of sections 1, 2, 3, 4, 5, 7, 9, 13, 15, 16 and 45 as a result of the implementation of the new biometric identity card and the powers granted for the collection and storage of personal biometric data.

For reasons which will become evident later in the judgment, we propose to deal, in the first place, with the provisions of the Constitution dealing with specific rights other than the alleged right to privacy, namely sections 4, 5, 7, 13, 15, 16 and 45 of the Constitution.

The alleged breach of the right to life protected by section 4 of the Constitution

Section 4(1) of the Constitution provides:

> "*No person shall be deprived of his life intentionally save in execution of the sentence of a Court in respect of a criminal offence of which he has been convicted.*"

Section 4(2) then enumerates four circumstances where a person shall not be regarded as having been "deprived of his life" in contravention of the section.

It is the contention of the plaintiff that the right to life subsumes the right to privacy. Counsel for the plaintiff has referred to Article 21 of the Constitution of India which provides that no person "*shall be deprived of his life .... except according to procedure established by law.*"

484

And he has pointed out that it has been held in the Indian case law that a scheme – The Aadhaar Scheme – whereby the applicants were required to part with personal information on biometrics, iris and fingerprints was in breach of Article 21 inasmuch as it infringed their right to privacy which was part of their right to life.

Counsel for the defendants has submitted, in reply, that there is nothing in plaintiff's evidence nor in the written submissions of plaintiff's Counsel, indicating how plaintiff's right to life is jeopardized.

In our view the reference to Article 21 of the Indian Constitution and to the record of proceedings of the Aadhaar case which was put in by Counsel for the plaintiff cannot be of assistance to the plaintiff's case inasmuch as section 4 of our Constitution cannot, having regard to its specific wording, be construed in the same way as Article 21 of the Indian Constitution. Indeed, the wording of section 4 of our Constitution makes it clear that the constitutional protection afforded is in respect of life in contradistinction from death. It is significant that all four circumstances set out under section 4(2) as those where a person shall not be regarded as having been deprived of his life in breach of the section relate to the person's death as a result of force that is reasonably justifiable for certain purposes. We consider therefore that the law for the implementation of the new biometric card and for the collection and storage of personal biometric data does not constitute a breach of the right to life protected by section 4 of the Constitution.

The alleged breach of the right to liberty as afforded by section 5 of the Constitution

The plaintiff is complaining that there is breach or likely breach of his right to liberty as afforded by section 5 of the Constitution.

Section 5(1) of the Constitution provides that "*No person shall be deprived of his personal liberty save as may be authorised by law*" in a number of circumstances listed (a) to (k).

The plaintiff has averred in that respect that *"the unilateral decision of Defendants of imposing a legal obligation upon him to submit his fingerprints and this, without his consent and further the collection, processing and/or retention of Plaintiff's personal biometric information including his fingerprints constitutes a serious interference by Defendants and/or their agents*

485

and/or their employees with Plaintiff's basic fundamental constitutional rights amongst the right to liberty and the right to protection of private life."

The plaintiff is also contending that "*The blanket power of collection and the indefinite storage of personal biometric data, including fingerprints, on the biometric identity card of citizens, including Plaintiff, are in breach of section 5 of the Constitution*".

Furthermore, the plaintiff is challenging the constitutionality of section 7(1) and (1A) of the National Identity Card Act as being violative of his fundamental right to liberty. It has been argued, in that connection, that the plaintiff has a serious apprehension that he will be legally compelled to show his biometric identity card on request by any person. He will thus be compelled to produce his card forthwith or within a reasonable time and there is no indication in the law as to who is authorized to ask for the production of his identity card and when.

The defendants' stand is that the question of plaintiff being deprived of his personal liberty does not arise at all. There is close similarity between section 5 of the Constitution and Article 5 of the European Convention, hence the propriety of referring to the jurisprudence on the European Convention. An overview of local jurisprudence as well as that of the European Court of Human Rights in relation to section 5 of the Constitution and to Article 5 of the European Convention reveals that the right to liberty being conferred is the right not to be detained physically either arbitrarily or unlawfully. The imposition upon the plaintiff of a legal obligation to allow his fingerprints to be taken does not amount to actual physical deprivation of the plaintiff's personal liberty. Nor do the collection and retention of fingerprints deprive the plaintiff of his physical liberty.

A careful examination of section 5 of the Constitution lends support to the stand of the defendants. The circumstances listed (a) to (k) in which the law may provide for the deprivation of a person's personal liberty make it clear that the protection which is afforded under section 5 is essentially in respect of the deprivation of the physical liberty of that person. Section 7(1) and (1A) of the National Identity Card Act only creates a legal obligation for a person to produce his National Identity Card. This can only be done according to the Act, upon a request made by a person who is empowered by law to ascertain the identity of a person in reasonable circumstances. Such a request does not amount, in our view, to any physical deprivation of a person's liberty as contemplated by section 5 of the Constitution. Similarly, the legal obligation created under section 4(2)(c) of the National Identity Card Act for a person to allow his fingerprints to be taken, and the provision under the Data Protection Act for the collection,

retention and storage of personal data cannot be said to amount to an actual physical deprivation of personal liberty in breach of section 5 of the Constitution.

The alleged breach of section 7 of the Constitution which provides protection from inhuman treatment

Section 7(1) of the Constitution provides:

"No person shall be subjected to torture or to inhuman or degrading punishment or other such treatment."

"*Inhuman*" in section 7 of the Constitution has been defined in **Virahsawmy and Anor v The Commissioner of Police [1972 SCJ 169]** (Sir Maurice Latour-Adrien CJ and Ramphul J.) as "*brutal, unfeeling, barbarous*". In the **Handbook issued by the Council of Europe on the Prohibition of Torture**, it is made clear that ill-treatment that does not have sufficient "*intensity or purpose*" to amount to torture, will be classed as "*inhuman*" or "*degrading*" when it deliberately causes "*severe suffering, mental or physical, which in the particular situation is unjustifiable*".

In the light of the above definitions, we agree with the submission of Counsel for the defendants that the plaintiff has failed to show how the collection and retention of fingerprints data amount to a breach or a likely breach of section 7 of the Constitution. Plaintiff has complained that he feels he is being treated as a criminal when he feels compelled, under penal sanction, to provide his fingerprints. However, as rightly pointed out by the defendants' Counsel in their written submissions, the plaintiff is wrongly associating the collection of fingerprints for the purpose of the NIC with the collection of fingerprints of people convicted of criminal charges or subject to criminal investigation. Fingerprints are collected and retained to allow identity authentication and to prevent usurpation of identity. Furthermore, they are provided to the Registrar of Civil Status in a conversion centre and not given in a police station in circumstances in which one is being treated as a suspect. The plaintiff has failed to establish that the taking of fingerprints or the procedure for the collection and storage of data prescribed under the Act and Regulations would subject the plaintiff "*to torture or to inhuman or degrading punishment*" in violation of section 7 of the Constitution.

The alleged breach of section 13 of the Constitution which provides for protection of freedom of assembly and association

Section 13(1) provides:

487

"Except with his own consent, no person shall be hindered in the enjoyment of his freedom of assembly and association, that is to say, his right to assemble freely and associate with other persons and, in particular, to form or belong to trade unions or other associations for the protection of his interests."

Section 13(2) then sets out the circumstances in which a law shall not be held to be inconsistent with or in contravention of this section.

In para 59 of plaintiff's written submissions, it is submitted that the implementation of the new biometric identity card scheme by the employees of defendants is in breach of section 13 of the Constitution; and that the blanket power of collection and the indefinite storage of personal biometric data, including fingerprints, on the biometric identity cards of citizens, including plaintiff, by the employees of defendants are also in breach of section 13 of the Constitution.

We however agree with the submission of Counsel for the defendants that in view of the plaintiff's broad and unsubstantiated submission at paragraph 59 of his written submissions, the plaintiff has not in any way shown how section 13 of the Constitution has been breached or is likely to have been breached in relation to him.

The alleged breach of the freedom of movement guaranteed by section 15 of the Constitution

Section 15(1) of the Constitution provides:

"No person shall be deprived of his freedom of movement, and for the purposes of this section, that freedom means the right to move freely throughout Mauritius, the right to reside in any part of Mauritius, the right to enter Mauritius, the right to leave Mauritius and immunity from expulsion from Mauritius."

Section 15(2) and (3) then provides in which circumstances restrictions on a person's freedom of movement shall not be inconsistent with or in contravention of this section.

We agree with Counsel for the defendants that no cogent submissions have been made on behalf of the plaintiff on the issue of breach of this section.

In the plaint with summons plaintiff has claimed that his freedom of movement is likely to be breached because it has been announced that persons above 60 years of age will have to show their new identity card whilst travelling by bus, and plaintiff will turn 60 next year. However as rightly pointed out by Counsel for the defendants, the above facts and the evidence of the

488

plaintiff do not disclose a breach or likely breach of plaintiff's freedom of movement, especially as there is no constitutional right to travel free by bus in Mauritius and, as per the evidence of Mr. Ramah, only the photograph on the card and the "SC" logo will be relevant for the purposes of bus travel. No contravention of the plaintiff's right to freedom of movement has been established.

The alleged breach of section 16 of the Constitution which offers protection from discrimination

Section 16(1) provides that no law shall make any provision that is discriminatory either of itself or in its effect. Section 16(3) defines "*discriminatory*" as meaning "*affording different treatment to different persons attributable wholly or mainly to their respective descriptions by race, caste, place of origin, political opinions, colour, creed or sex.*" Sections 16(4), (5) and (7) then provide in which circumstances a law shall not be held to be inconsistent with or in contravention of this section.

As rightly submitted by Counsel for the defendants, the plaintiff has not made out any case for a breach or likely breach of section 16 of the Constitution.

The alleged breach of section 45 of the Constitution

Section 45 provides that "*subject to this Constitution, Parliament may make laws for the peace, order and good government of Mauritius*".

The Mauritian Parliament is thus vested with exclusive power to pass any laws which in its wisdom will promote "*peace, order and good government,*" and the only limitation to this power is that it must not be exercised in breach of the Constitution. The role of the Court is therefore to decide on the constitutionality of any law enacted by Parliament and the Court's intervention falls squarely within the ambit of section 2 of the Constitution which reads:

> "*This Constitution is the supreme law of Mauritius and if any other law is inconsistent with this Constitution, that other law shall, to the extent of the inconsistency, be void*".

As the only arguments of the plaintiff in relation to section 45 of the Constitution question issues of policy and good governance generally including disbursement of allegedly excessive funds, and do not indicate any specific breach of the Constitution in the exercise of the Constitutional law making powers under section 45, we do not consider that our intervention as a constitutional Court is warranted.

489

The alleged breaches of constitutional provisions relating to privacy

We now turn to the constitutional provisions which are alleged to confer a right of privacy and the legislative provisions which are alleged to be violative of that right.

The relevant provisions of the National Identity Card Act ("NIC Act")

There is a legal duty on every adult citizen of Mauritius to apply for the issue of an identity card under Section 4 of the NIC Act.

For that purpose section 4(2) provides that:

"2. *Every person who applies for an identity card shall –*

(a) *produce his birth certificate or his certificate of registration or naturalisation as a citizen of Mauritius, as the case may be;*

(b) *produce such other documents as the Registrar may require;*

(c) *allow his fingerprints, and other biometric information about himself, to be taken and recorded; and*

(d) *allow himself to be photographed;*

for the purpose of the identity card."

"Biometric information" is defined in section 2, which is the Interpretation section of the Act, in the following terms:-

"biometric information" in relation to an individual, means data about his external characteristics, including his fingerprints;"

Section 5(2)(h) further provides that every identity card shall contain, in electronic form or otherwise "*such other information as may be prescribed*".

Section 7 deals with the requirement to produce an identity card when requested. Section 7(1) of the Act provides as follows:

"7. *Production of identity card*

(1) Every person may –

(a) in reasonable circumstances and for the purpose of ascertaining the identity of another person; or

490

(b) where he is empowered by law to ascertain the identity of another person,

request that other person to produce his identity card where that person is a citizen of Mauritius."

Section 7(1A) of the NIC Act further provides as follows:

"(1A) Where a person is required to produce his identity card in accordance with subsection (1)(b), he shall –

(a) forthwith produce his identity card to the person making the request; or

(b) *where he is not in possession of his identity card, produce his identity card within such reasonable period, to such person and at such place as may be directed by the person making the request."*

Section 3 of the Act provides that the Registrar of Civil Status shall cause to be kept a register in which shall be recorded particulars of the identity of every citizen of Mauritius. Section 3(2)(b) reads as follows:

"3(2) *The particulars required to be recorded in respect of any person under subsection (1) shall be –*

(a) the sex and names of that person; and

(b) such other reasonable or necessary information as may be prescribed regarding the identity of the person."

Section 10 of the Act empowers the Minister responsible for the subject of Civil Status to make such Regulations as he deems necessary for the purposes of the Act.

Section 9(2) and (3) of the Act provides that any person who contravenes the Act, or any regulations made under it, shall commit an offence for which he or she shall be liable, on conviction, to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.

Section 12 of the Act further provides that the collection and processing of personal data, including biometric information under the Act shall be subject to the provisions of the Data Protection Act.

491

The National Identity Card (Particulars in Register) Regulations 2013 made pursuant to sections 3(2)(b) and 10 of the NIC Act, prescribe the particulars to be included in the Register. Regulation 3 reads as follows:

> "3. *For the purposes of Section 3(2)(b) of the Act, the following particulars of a person shall be recorded in the register –*
>
> ... ...
>
> *(f) fingerprints; and*
>
> *(g) encoded minutiae of fingerprints."*

The Constitution

We need to consider in the first place whether the legislation breaches any of the fundamental rights of the plaintiff invoked by him.

Before the issue can be addressed it is necessary to consider the essential characteristics and functions of our Constitution. These were conveniently set out and explained in **Ahnee v Director of Public Prosecutions [1999] 2 AC 294, 302-3** and cited with approval in **The State v Khoyratty [2006] UKPC 13**:

(a) Mauritius is a democratic state based on the rule of law.

(b) The principle of separation of powers is entrenched.

(c) One branch of government may not trespass on the province of any other in conflict with the principle of separation of powers.

Subject to the Constitution, the sole legislative power is vested in Parliament (Section 45). But the Constitution being the Supreme law of Mauritius, any law which is inconsistent with the Constitution should to the extent of its inconsistency with any of the provisions of the Constitution be declared void by the Supreme Court [section 2].

The Supreme Court is vested under sections 17 and 83 of the Constitution with wide constitutional powers to enforce protection of any of the Constitutional rights of a citizen.

Whilst Chapter I of the Constitution provides that Mauritius shall be a sovereign democratic state, Chapter II goes on to spell out the provisions guaranteeing the protection of fundamental rights and freedoms of the individual. The plaintiff has invoked a breach of several of these fundamental rights which include sections 3, 4, 5, 7, 9, 13, 15 and 16 of the Constitution.

Much emphasis has been laid, however, by the plaintiff, on sections 3 and 9 of the Constitution and Article 8 of the European convention which, it has been submitted, establish a constitutionally protected right to privacy and private life.

It has been submitted on behalf of the defendants that the protection offered by sections 3 (c) and 9 of the Constitution cannot be interpreted as affording a general right to privacy or private life for the following reasons:

(1) The framers of our Constitution have clearly departed from the wording of Article 8 of the European Convention although it is generally accepted that the Chapter II rights of the Mauritian Constitution have been modelled on that Convention and had they intended to adhere to the provisions of that article they would have expressly done so as has been done in other Commonwealth Constitutions.

(2) The wording used in the European Convention is different from that used in sections 3 (c) and (9) of the Constitution of Mauritius: therefore it cannot be assumed that sections 3(c) and (9) of the Constitution were meant to confer a general right to privacy.

(3) Even though constitutional provisions are generally given a generous and purposive interpretation, wholesale articles from the European Convention cannot be blindly imported into the Constitution of Mauritius.

(4) The Judicial Committee of the Privy Council in **Matadeen v Pointu** [1998 MR 172] points out that the case of the **Société United Docks v Government of Mauritius [1985] AC 585** is only authority for the principle that section 3 of the Constitution is a *"freestanding enacting section which has to be given effect in accordance with its terms"*. The Judicial Committee stressed that the words of section 3 of the Constitution should be given their natural and ordinary meaning and section 3 should not be construed as creating rights which it does not contain.

(5) As opposed to those countries where the right to privacy or the respect for one's private life is constitutionally entrenched, in Mauritius the right to privacy is not provided for in the Constitution, but in article 22 of the Civil Code: see **Soornack v Le Mauricien & Ors** [2013 SCJ 58]. It is also secured through the Data Protection Act. This means that the right may be limited, modified or varied by a subsequent statute.

On the other hand, it has been strongly argued on behalf of the plaintiff that there is a constitutionally protected right to privacy and private life as a result of which the provisions of

493

the law for the exercise of taking fingerprints as well as the processing and retaining of the personal data of the plaintiff would violate his fundamental rights.

It is not in dispute that the biometric concept involves the extracting of *minutiae* from the fingerprints of the plaintiff which will be finally recorded and stored in a database. The exercise is in distinct phases. The plaintiff must first allow for the taking of his fingerprints. The data obtained are then processed and encoded in his identity card. Subsequently, the data prescribed under regulation 3 of the National Identity Card (Particulars in Register) Regulations 2013 are retained and stored in a register kept and managed by the Registrar of Civil Status.

One of the first questions which therefore arises at this juncture is whether the taking of the plaintiff's fingerprints would in such circumstances constitute a breach of any of his fundamental rights protected under the Constitution. It is the plaintiff's case that the taking of fingerprints against his will breaches his right to privacy, which is afforded entrenched constitutional protection under Sections 3 and 9 of the Constitution. The relevant parts of Section 3 and 9 read as follows:

> *"3. Fundamental rights and freedoms of the individual*
>
> *It is hereby recognized and declared that in Mauritius there have existed and shall continue to exist without discrimination by reason of race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, each and all of the following human rights and fundamental freedoms –*
>
> (a) *the right of the individual to life, liberty, security of the person and the protection of the law;*
>
> *(b) freedom of conscience, of expression, of assembly and association and freedom to establish schools; and*
>
> (c) *the right of the individual to protection for the privacy of his home and other property and from deprivation of property without compensation*
>
> *9. Protection for privacy of home and other property*
>
> *(1) Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises."*

It was incumbent upon the framers of our democratic constitution to determine to what extent they would entrench in our Constitution the protection for the privacy of the individual. Firstly, as regards Section 3, an analysis of the precise words used in Section 3(c) tends to show that the protection does not extend to the physical privacy of a person. The words used are "*the right of the individual to protection for the privacy of*

494

his home and other property". Section 3 does not therefore contain words or terms which confer a right to the privacy of the person and which may encompass any protection against the taking of fingerprints from a person. Section 3 thus appears to afford protection only for the privacy of a person's home and property.

The case of **The Société United Docks and Others v The Government of Mauritius [1982] PRV 34** is authority for the principle that Article 3 is not a mere preamble but is a "*freestanding enacting section which had to be given effect in accordance with its terms*".

But as was highlighted by the Judicial Committee of the Privy Council in Matadeen v Pointu. [1998 MR 172], section 3 or the subsequent sections of the Constitution cannot be interpreted as creating rights which they do not contain. The relevant part of the judgment reads as follows:

> "*Their Lordships have already made reference to the previous decision of the Board in the Société United Docks v. Government of Mauritius [1985] A.C 585.*
>
> *[...]*
>
> *Their Lordships do not regard this case as deciding more than that the words of section 3 should be given their natural and ordinary meaning and that they should not be artificially restricted by reference to subsequent sections, even though the latter are said to have effect for the purpose of affording protection to the rights enumerated in section 3. The Board said in its opinion that 'a Constitution concerned to protect the fundamental rights and freedoms of the individuals should not be narrowly construed in a manner which produces anomalies and inexplicable inconsistencies.'*
>
> *Their Lordships would not wish in any way to detract from this statement of principle but it cannot mean that either section 3 or the later sections can be construed as creating rights which they do not contain.*"

The language of Section 3(c) of the Constitution, construed in the light of its natural and ordinary meaning, does not create or confer any right of privacy to the person and would not, in the present matter, afford constitutional protection against the taking of fingerprints as prescribed under the NIC Act and Regulations.

Furthermore, the provisions of Sections 3 and 9 of our Constitution are not the equivalent of Article 8 of the European Convention and would not as a result create constitutionally protected rights of privacy and private life in the same manner and to the same extent as Article 8 of the European Convention ("The Convention"). It is apposite to set out here Article 8 of the Convention:

"ARTICLE 8

495

Right to respect for private and family life

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

Among the interests protected by Article 8 is the right to respect for private life. Indeed, in the decision in **S v United Kingdom [2009] 48 E.H.R.R 50** – on which the plaintiff relies – the European Court of Human Rights "*recalls that the concept of 'private life' is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person. It can therefore embrace multiple aspects of the person's physical and social identity.*" [paragraph 66].

The Court states in no uncertain terms that the right protected is one to "*respect for private life*". Thus it states as follows at paragraph 68:

> *"The Court notes ..... that all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals."*

And it expresses the following view at paragraph 84:

> *".....fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life ....."* (emphasis added)

Similarly in the recent decision of the Strasbourg Court in **Michael Schwarz v Stadt Bochum** handed down on 17 October 2013, the issue considered by the Court is *"whether taking fingerprints and storing them in passports.....constitutes a threat to the rights to respect for private life..... If so, it must be ascertained whether such a threat can be justified."* [paragraph 24]. This indicates that the decisions of the European Court of Human

496

Rights are based on the protection of a right to respect for private life, which protection is not afforded by the wording of sections 3 and 9 of our Constitution.

Accordingly, the numerous cases referred to by the plaintiff, which are based on Article 8 of the Convention, would not readily find their application in view of the difference in the wording of that article when compared with Section 9 of our Constitution.

We may here refer to the approach adopted in that connection in interpreting the Constitution with regard to the protection of fundamental rights guaranteed under Chapter II. The Court in **Union of Campement Sites Owners and ors. v The Government of Mauritius [1984] MR 100** pointed out the following:

> *"Constitutional instruments, however, differ in their formulation, reflecting the measure in which individual, collective or institutional rights are designed to be safeguarded."*

The Court added, with reference to some provisions of The American and Indian Constitutions which had been invoked in the interpretation of fundamental rights under our Constitution –

> *"that Constitutions are formulated in different terms and must each be read within its own particular context and framework. The American and Indian Constitutions were drafted in a different age and have tended, particularly with regard to fundamental freedoms of the individual and to a greater extent than more modern Constitutions, to make broad and wide ranging formulations which have necessitated a number of amendments and specific derogations or else have required recourse to implied concepts of eminent domain or police powers in order to keep literal interpretations of individual rights within manageable limits. We should be very cautious, therefore, in importing wholesale into the structure and framework of our constitution a complete article of the kind that Article 14 of the Indian Constitution or the 14th Amendment of the American Constitution are, the more so, as section 111(2) of our Constitution requires us to look to the interpretation Act of 1889 for the purpose of construing our Constitution. We would, therefore, seek to confine ourselves to the substantive provisions of our Constitution and only go outside them, or even to the marginal notes, in the case of some patent ambiguity."*

The plaintiff also relies on what was stated in **Hurnam v The State [2005] UKPC 49**:

> *"It is indeed noteworthy that the European Convention was extended to Mauritius while it was still a Crown Colony, before it became independent under the 1968 Constitution: see European Commission of Human Rights, Documents and Decisions (1955 – 1957), p 47. Thus the rights guaranteed to the people of Mauritius under the European Convention were rights which, on independence, 'have existed and shall continue to exist' within the terms of section 3. This is a matter of some significance: while Mauritius is no longer a party to the European Convention or bound by its terms, the Strasbourg jurisprudence*

497

gives persuasive guidance on the content of the rights which the people have enjoyed and should continue to enjoy."

But this statement must be viewed in its context. The Judicial Committee was in the process of examining section 5(1) and (3) and section 10(2)(a) of our Constitution and had expressly observed that:

"Section 5(1) and (3) and Section 10(2)(a) bear a very close resemblance to articles 5(1) and (3) and 6(2) of the European Convention on Human Rights."

The Strasbourg jurisprudence therefore gives persuasive guidance on the contents of the fundamental rights embodied in Chapter II of our Constitution in respect of those rights which are couched in terms which bear very close resemblance to the corresponding articles of the European Convention on Human Rights.

We need to observe in this respect that the provisions of section 9 of our Constitution do not bear close resemblance to the detailed provisions of article 8 of the Convention. Furthermore, whilst article 22 of our Civil Code provides for a right to the protection of private life (*"Chacun a droit au respect de sa vie privée"*), that article does not have the status of a constitutional right and cannot fetter the law making powers of the legislature in enacting any other legislation.

We need therefore to turn to the substantive provisions of our Constitution in order to determine the scope of constitutional protection which is afforded to the citizens of Mauritius in respect of their fundamental rights to privacy. We have already seen that the wording of Section 3 of the Constitution, when construed in the light of its natural and ordinary meaning would not afford constitutional protection against the taking of fingerprints. We are left to consider Section 9 of the Constitution. We need to reproduce in that respect the material part of Section 9(1) in order to carry out a close scrutiny of its wording and provisions which unlike Section 3, also includes protection in respect of the privacy of a person.

"9. *Protection for privacy of home and other property*

(1) *Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises."*

For the purposes of the present case, the key words are that no person shall be subjected to the search of his person except with his own consent.

Every adult citizen of Mauritius is bound to apply for a National Identity Card and is mandatorily required, under Section 4(2) of the Act, *"to allow his fingerprints, and other biometric information about himself to be taken and recorded"*. The coercive nature of this

obligation is further highlighted by the criminal sanction provided under section 9, in case of any failure by a citizen to comply with these provisions of the Act. The citizen is therefore under an obligation by virtue of these legal provisions to allow his fingerprints to be taken and recorded in conformity with the Act and Regulations. He is under compulsion to submit his fingers to the relevant authorities for the extracting of minutiae from his fingerprints in order to enable those authorities to record in the Register the encoded minutiae of his fingerprints. The evidence has indisputedly shown that the "*minutiae*" which are recorded from the fingerprints contain unique personal data peculiar to each individual.

The next question is whether, in view of the highly personal and private nature of fingerprints which contain sensitive personal information about an individual, the coercive act of taking his fingerprints would tantamount to a breach of the protection of his Constitutional right to privacy within the ambit of Section 9(1) of the Constitution. In other words, would this coercive act of the "*taking of fingerprints*" against the will of a citizen fall within the purview of a citizen being "*subjected to the search of his person*" as contemplated by Section 9(1) of the Constitution?

It is axiomatic that we should remind ourselves at this juncture of the sacrosanct rules of interpretation which apply to the construing of the wording of the Constitutional provisions which create and consecrate the fundamental human rights of the citizens of Mauritius under Chapter II of our Constitution. There is ample authority to support the view that a written Constitution should not be looked upon as an Act of Parliament, but rather as a charter or a covenant which must be given a generous and purposive interpretation. **[Olivier v Buttigieg (1967) A.C. 115; Ong Ah Chuan v Public Prosecutor (1981) A.C. 648; Attorney-General of The Gambia v Momodou Jobe (1984) A.C. 689, 700]**. The constitutional provisions enshrining fundamental rights "*call for a generous interpretation avoiding what has been called the 'austerity of tabulated legalism', suitable to give to individuals the full measure of the fundamental rights and freedoms referred to*" **[Minister of Home Affairs v Fisher (1980) A.C. 319 (PC)]**.

The language used in section 9(1) no doubt seeks to afford purposive constitutional protection to the private physical integrity of a person against any form of search. In that connection, the protection is obviously not limited to a search of the whole body of a person. The search of any part of the body of a person would fall within the scope of the protection afforded by section 9(1). The protection may even extend further than that. Indeed, for instance, the search of the pocket of a garment being actually worn by a person cannot be excluded from the purview of a search of a person under section 9(1).

499

A purposive interpretation would not be confined to the giving of a narrow and restrictive meaning to the word "*search*" as used in section 9(1) of the Constitution. Any undue intrusion or any examination or inspection of any part of the body of a person would thus, in our view, fall within the purview of a search of a person for the purposes of section 9(1).

We are not here for that purpose concerned with the degree of intrusiveness but with a fundamental right of the protection of the privacy and integrity of the body of a person. The protection under section 9(1) would clearly be against any form of undue interference by way of a search of any part of the body of a person without his consent. The coercive taking of fingerprints from the fingers of a person and the extracting of its *minutiae* would thus clearly fall within the scope of the protection afforded to the integrity and privacy of the person under Section 9(1) of the Constitution.

We hold therefore that the provisions of the NIC Act and Regulations which enforce the compulsory taking and recording of fingerprints of a citizen of Mauritius disclose an interference with the plaintiff's right against the search of his person guaranteed under Section 9(1) of the Constitution.

We feel comforted in our view by the pronouncements in Payet v Seagull Insurance Co Ltd and Ors [1990 SCJ 282] and the Canadian case of Michael Feeney v Her Majesty the Queen [1997 2 SCR 117].

In Payet (*supra*), Yeung Sik Yuen J. stated:

> *"Now, Chapter II of our Constitution which deals with the protection of fundamental rights and freedoms of the individual inter alia provides for the right of the individual to protection for the privacy of his home and other property (including his body) and also for the protection of his right to personal liberty. One cannot think of a case where the protection of fundamental rights and freedoms of the individual can be more sacrosanct than where the protection relates to the body of the individual." (Emphasis added)*

In Michael Feeney (*supra*), Mr. Feeney was suspected of having committed a criminal offence. He was arrested and his fingerprints were taken by the authorities. Section 8 of the Canadian Charter of Rights and Freedoms states: "*Everyone has the right to be secure against unreasonable search or seizure.*" In interpreting that section, the Supreme Court of Canada held that "*compelling the accused to provide fingerprints in the present context*" was "*a violation of section 8 of the Charter, involving as it did a search and seizure related to the appellant's body, about which, at least in the absence of a lawful arrest, there is a high expectancy of privacy*".

500

We note that section 9 (1) of our Constitution is couched in wider terms than section 8 of the Canadian Charter inasmuch as section 9(1) affords protection against any form of coercive bodily search whilst the protection afforded under section 8 of the Canadian Charter is in respect of any "unreasonable" search of the person.

The permitted derogation from the right under section 9(2) of the Constitution

However, the right which exists under section 9(1) of the Constitution for a person not to be subjected to bodily search except with his consent is not an absolute one. A limitation to that right is permissible under section 9(2), the relevant part of which reads as follows:

> *"9 Protection for privacy of home and other property*
>
> [.....]
>
> (2) *Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision --*
>
> *(a) in the interests of ..... public order .....;*
>
> *(b) for the purposes of protecting the rights or freedoms of other persons;*
>
> [.....]
>
> *except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society."*

A limitation to the right not to be subjected to bodily search is therefore permissible, under section 9(2), in the case of a provision made by a law in the interests of, *inter alia*, public order. The exception prescribed under section 9(2) would however be permissible, in the words

501

at the end of section 9, "*except so far as that provision or as the case may be the thing done under its authority, is shown not to be reasonably justifiable in a democratic society*".

Do the acts purporting to affect the rights of the plaintiff under section 9(1) of the Constitution constitute permissible derogations "in the interests of public order" under section 9(2) of the Constitution?

The wording of section 9(2) invites us to consider in the first place whether the impugned acts are done "*under the authority of any law*".

We may usefully refer for that purpose to the following passages from the decision of the European Court of Human Rights in **Leela Förderkreis E.V. v Germany (2009) 49 E.H.R.R. 5.**

> *"113. The Court reiterates its settled case-law that the expression 'prescribed by law' requires firstly that the impugned measure should have a basis in domestic law. It also refers to the quality of the 'law' in question, requiring that it be accessible to the persons concerned and formulated with sufficient precision to enable them – if need be, with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail and to regulate their conduct* (Gorzelik and Others v Poland [GC], No. 44158/98, § 64, ECHR 2004 1)
>
> *Further, as regards the words 'in accordance with the law' and 'prescribed by law' which appear in Articles 8 to 11 of the Convention, the Court observes that is has always understood the term 'law' in its substantive" sense, not its 'formal' one (De Wilde, Ooms and Versyp v Belgium, judgment of 18 June 1971, Series A no. 12, P.·45 § 93). 'Law' must be understood to include both statutory law and judge-made 'law' (see, among other authorities, The Sunday Times v the United Kingdom (no. 1), judgment of 26 April 1979, Series A no. 30, p. 30, § 47, and Casado Coca v Spain, judgment of 24 February 1994, Series A no. 285-A, P. 18, § 43). In sum, the 'law' is the provision in force as the competent courts have interpreted it."*

We consider that these conditions are met by the "law" which has been enacted in that respect.

The provisions of the law limiting the right of the plaintiff to refuse to allow his fingerprints to be taken, by availing himself of his right under section 9(1) not to be subjected to a search of his person except with his consent, are section 4(2)(c) of the NIC Act (*supra*) and the Regulations made in that connection. Section 4(2)(c) provides that every person who applies for an identity card shall "*allow his fingerprints and other biometric information about himself to be taken and recorded ... for the purpose of the identity card.*"

502

The next question which arises is whether that provision has been made in the interests of public order and whether such interference with the right under section 9(1) is justifiable. The defendants have adduced evidence in that connection.

Mr. Gunputh Rao Ramah, the project director of the Mauritius National Identity Scheme (MNIS) project gave explicit details to show what make fingerprints particularly reliable as a means of identifying or authenticating the identity of persons, hence giving an added dimension to the new identity card. Once the fingerprints have been captured, they can be used for verification purposes. He gave the following example:

> *"What happens is when a person comes to the registration centre, the fingerprints are captured. When the person comes to collect the card, the fingerprints of the person are verified against what is on the card and this is a very reliable way of actually telling if it is this person coming to collect or not."*

The great advantage of using fingerprints for identification purposes is that a person's fingerprints are unique to him and will not even be the same as those of his identical twin. Mr. Ramah has also explained how the use of fingerprints has enabled the detection and prevention of multiple enrolments:

> *"We have identified more than 700 people who have tried to register more than once. In fact they went to one centre, possibly went to a different centre ... when the system analyses the fingerprints, the system flags these people as being those who tried to register twice on the same identity card for example and then there is an investigation that happens afterwards."*

The evidence of Mr Ramah has brought into focus the serious flaws inherent in the previous system and which could give rise to identity fraud. Furthermore, the previous system could not effectively prevent the issue of an identity card with the same national identity number to more than one person. On the other hand it has been amply shown that the new system is the only system which can provide effective safeguards against identity fraud and cater for identity authentication not only at the time of the issuing of a new card but also in case of renewal of a card or issue of a replacement card.

Mr. Goparlen Pavaday, Project Manager and Head of Operation of the MNIS, further highlighted the security features inherent in the new system as opposed to any other alternative system. He also explained that the authentication process through the taking of fingerprints is vital in order to prevent identity usurpation and ensure that every citizen has a unique identity

503

and a unique identity card. He also pin-pointed the importance of the speed and accuracy of the authentication process which would be higher with ten instead of four fingerprints.

The evidence of Mr. Ramah and Mr. Pavaday in relation to the importance of fingerprints has hardly been challenged and their testimonies have provided compelling reasons to establish that the law providing for the taking of fingerprints is fully justifiable on the grounds of public interest and public order.

We accordingly conclude that the provision in section 4(2)(c) of the NIC Act and the Regulations made under that Act have been made in the interests of public order and constitute a justifiable interference with the right of the plaintiff against the search of his person as provided for under section 9(1) of the Constitution.

Has the provision in section 4(2)(c) been shown not to be reasonably justifiable in a democratic society?

Although it has been submitted by the plaintiff that the imposition of a legal obligation upon him to submit his fingerprints without his consent would not be reasonably justifiable in a democratic society, no cogent argument has been presented before us in support of such a contention. The burden of proving that the act complained of is not reasonably justifiable in a democratic society lies on the plaintiff.

The relevant test in that connection has been laid down by the European Court of Human Rights in the case of **S and Marper v the United Kingdom [2008] ECHR 1581** (Applications Nos. 30562/04 and 30566/04 – 4 December 2008). At paragraph 101 of that judgment we read the following:

> *"An interference will be considered 'necessary in a democratic society' for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reason adduced by the national authorities to justify it are 'relevant and sufficient'."*

Furthermore, as was pointed out by the European Court of Human Rights in **Sahin v Turkey (2005) 41 E.H.R.R.8**, in order to assess the "necessity" for interference,

> *"103..... the Court's task is confined to determining whether the reasons given for the interference were relevant and sufficient and the measures taken at the national level proportionate to the aims pursued."*

504

Applying the above test to the facts of the present case, we find that it can hardly be disputed that the taking of fingerprints within the applicable legal framework pursues the legitimate purpose of establishing a sound and secure identity protection system for the nation and thus answers a pressing social need affording indispensable protection against identity fraud. Such a purpose, as has been amply demonstrated, is vital for proper law enforcement in Mauritius. Furthermore, taking into consideration the appropriate safeguards in the taking of fingerprints for their insertion in the cards, and the relatively limited degree of interference involved, we are led to conclude that such interference is proportionate to the legitimate aim pursued.

In the light of our above observations we conclude that the plaintiff has failed to discharge the burden of showing that the interference in question is not reasonably justifiable in a democratic society.

We shall now turn to the issue of the storage and retention of personal biometric data.

The issue of storage of personal biometric data including fingerprints

The relevant law

As we have seen above there is, in section 9(2) of the Constitution, a permissible derogation from the right protected under section 9(1). Section 9(2) indeed provides that "*Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision – (a) in the interests of ... ... public order ...*" (emphasis added).

It has been submitted on behalf of the plaintiff that no such law has been enacted to provide for the storage of fingerprints and other personal biometric data such that the derogation under section 9(2) is simply not applicable.

On the other hand, it has been submitted on behalf of the defendants that the retention of fingerprints and other personal biometric data has been done under the authority of the law given that such retention is prescribed in section 3 of the National Identity Card Act and the National Identity Card (Particulars in Register) Regulations 2013.

Section 3(1) of the Act provides for the keeping of a register "*in which shall be recorded particulars of the identity of every citizen of Mauritius*". Section 3(2)(b) goes on to provide that the particulars required to be recorded in section 3(1) shall include "*such other reasonable or necessary information as may be prescribed regarding the identity of the person*". Regulations have been made to provide for the particulars of a person which shall be recorded in the register

505

for the purposes of section 3(2)(b) of the Act. Those particulars include, *inter alia*, the "*photograph*", the "*fingerprints*" and the "*encoded minutiae of fingerprints*".

In the light of the above enactments, we agree with Counsel for the defendants that there is a law providing for the storage and retention of fingerprints and other biometric data regarding the identity of a person.

Is the law in question a permissible derogation under section 9(2)?

The next question we have to answer is whether the law in question makes provision in the interests of public order such as to fall within the derogation permitted by section 9(2) of the Constitution.

For reasons similar to those on which we have based ourselves to answer this question in the affirmative in relation to the law providing for the taking of fingerprints, and which have already been spelt out earlier in this judgment, we also consider that there is a public order justification for the storage and retention of a person's fingerprints and other biometric data.

"Reasonably justifiable in a democratic society"

We have already set out, earlier, the legal principles which are applicable in order to determine whether the provisions of a law are reasonably justifiable in a democratic society. We now have to apply those principles in order to determine whether the law providing for storage and retention of a person's fingerprints and other biometric data are reasonably justifiable in a democratic society. As noted earlier, the relevant legal principles have been aptly summarized in **S and Marper v The United Kingdom** (*supra*) at paragraph 101. The first sentence of that paragraph reads:

> *"An interference will be considered 'necessary in a democratic society' for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'."*

We have already explained why it does appear to us that there is a "*pressing social need*" for the implementation of a national identity card system based on the taking of fingerprints. For similar reasons, we consider that the retention and storage of biometric data would answer a pressing social need in the pursuance of a legitimate aim, namely protection against identity fraud.

506

However, there are highly disturbing questions which arise concerning the system and legal framework which are applicable for the retention and storage of biometric personal data for an indefinite period. It is highly questionable whether the relevant laws and existing legal framework provide sufficient guarantees and safeguards for the storage and retention of personal biometric data and whether in the present circumstances they would constitute an interference proportionate to the legitimate aim pursued.

In the present matter, the plaintiff is under the legal obligation to apply for a new biometric card fitted with an electronic chip. The plaintiff is compelled to give his ten fingerprints which will be stored for an indefinite duration in a central data base in accordance with the Data Protection Act. The minutiae of four fingers are recorded in the electronic chip contained in the card.

Witness Sookun gave expert evidence on behalf of the plaintiff as to the various types of risks and dangers to which the plaintiff will be exposed in this era of cyber hacking, email hacking and bank account hacking, the more so since no such information system and no database is foolproof and the new identity card can be read at a distance with available technological devices.

Witness Sookun gave various illustrations of how access can be gained to personal data via Government websites including the MNIC website. He added that after carrying out tests on the government email, he was led to the conclusion that the government email with the extension "@mail.gov.mu" lacks security features, can be cloned and is open to abuse. He went on to explain that it is possible to have access to the MNIS database through a proxy attack – which is an indirect attack – via the government portal. He mentioned various tools that can be used to identify all the other machines which are in the internal network, one of which will have to be the MNIS. He also laid stress on the fact that when data is uploaded on a server a copy of the data remains on the local machine unless and until the data is deleted on the local machine.

The witness also referred to the dangers of having a centralized database which makes counterfeiting easier. According to him there is no database which is foolproof to cyber criminals. Furthermore there are no sufficient security features present at the Civil Status division.

Apart from the above facts there exists, according to the witness, the potential for an overwhelming risk of abuse and misuse of the plaintiff's personal data inasmuch as :-

507

(i) in view of the rapid technological development in the field of information technology, there is a serious risk that in future the private life interests bound up with biometric information may be adversely affected in novel and unpredictable ways;

(ii) the MNIS database may well be connected to the internet at a later stage;

(iii) the physical security measures presently available at the MNIS Data Centre at Ebene – where all the data are stored – are inadequate in that the data base works on a network system of people and devices which is not totally secure;

(iv) the personal data of individuals with no criminal record will be retained indefinitely in the same way as the personal data of convicted persons.

On the other hand, the defendants have advanced a number of reasons in support of their contention that the legal framework and MNIC system for the storage and retention of data are reasonably justifiable in a democratic society. It has been submitted that the reasons advanced to justify the implementation of such a system are proportionate to the legitimate aim pursued. The retention of the data is said to be essential for the prevention of multiple enrolments and for identity authentication at the time of issuing a new card or a replacement card, or in case of renewal. Both Mr Ramah and Mr Pavaday have emphasised that the retention of the data is vital to the authentication process in order to prevent identity usurpation and ensure that every citizen has a unique identity and a unique identity card. They added that there are no satisfactory alternatives to the present system based on the storage and retention of the biometric personal data.

We have examined with much attention the evidence of both witnesses Ramah and Pavaday. Although their testimonies might indicate that there is a legitimate aim for storing and collecting personal biometric data, we do not find that there have been sufficiently strong reasons advanced to establish that such storage and retention of data for an indefinite period is proportionate to the legitimate aim pursued. On the other hand, witness Sookun has said enough to impress upon us the risks and damages which the storage and retention system adopted by the defendants would entail.

We now need to turn to the relevant legal provisions which have been enacted in connection with the retention and storage of personal data in order to determine whether those legal provisions are, in the present circumstances, reasonably justifiable in a democratic society.

508

Section 3 of the NIC Act provides that the Registrar of Civil Status shall cause to be kept a register in which shall be recorded particulars of the identity of every citizen of Mauritius.

Section 12 of the NIC Act provides that the collection and processing of personal data, including biometric information, under that Act shall be subject to the provisions of the Data Protection Act.

Under section 24(1) of that latter Act, no personal data shall be processed unless the express consent of the data subject has been obtained. However, that Act contains a number of permissible derogations from that rule.

First, section 24 (2) of the Data Protection Act provides that personal data may be processed without the express consent of the data subject where, inter alia, the processing is necessary *"for the performance of a contract to which the data subject is a party"*, *"for compliance with any legal obligation to which the data controller is subject"* and *"in the public interest"*.

Second, Part VII of that Act provides for a number of further exemptions from any of the provisions of the Act which would enable persons other than the data subject to obtain his personal data from the data base. Under section 45, such personal data become accessible where in the opinion of the Prime Minister they are required for the purpose of safeguarding national security. Under section 46 personal data may also be made available where the processing of personal data is required for the purposes of *"the prevention or detection of crime"*, *"the apprehension or prosecution of offenders"* on *"the assessment or collection of any tax, duty or any imposition of a similar nature."* Under section 47, there can be access to the personal data where such access is being sought in relation to *"the physical or mental health of the data subject"*. Under section 48, the personal data are also made accessible to the Bank of Mauritius, the Financial Services Corporation and the Financial Intelligence Unit in their discharge of any statutory function. Section 48 also allows for the processing of personal data for the purpose of the discharge, by other bodies, of relevant functions for protecting members of the public against financial loss or dishonest or incompetent practices, or against risk to health or safety. Under section 49 processing of personal data is made permissible for journalistic, literary and artistic purposes, albeit under certain conditions. Under section 53, it is further provided that personal data may be made available *"where the data consist of information in respect of which a claim to legal professional privilege or confidentiality as between client and legal practitioner could be maintained in legal proceedings, including prospective legal proceedings."*

509

By virtue of section 52, there can be access to personal data where –

> "*(i) the disclosure of such data is required under any enactment or by a Court Order;*
>
> *(ii) the disclosure of such data is necessary for the purpose of, or in connection with, any on-going or prospective legal proceedings;*
>
> *(iii) the disclosure of such data is necessary for the purpose of obtaining legal advice; or*
>
> *(iv) the disclosure is otherwise necessary for the purpose of establishing, exercising or defending legal rights"*

The above survey of the legal exemptions makes it manifestly clear that the personal data of individuals such as the plaintiff can be readily accessed in a large number of situations. What is even more alarming is the relatively low threshold prescribed for obtaining access to personal data. A striking illustration of that is the enactment in section 52 (iii) (*supra)* whereby access may be obtained merely by invoking that the disclosure of the data is necessary for the purpose of obtaining legal advice.

What is even more objectionable is the absence of any safeguard by way of judicial control to monitor the access to personal data. The only instance where a Court Order is mentioned is under section 52 (i) (*supra)* and here too the basis upon which a Court Order may be granted is not set out at all.

It is a fundamental principle of the rule of law that there can be no interference with the legal or constitutional rights of a citizen except on recognized permissible grounds which require judicial control and sanction. This fundamental principle is well anchored in our legal traditions and framework. By way of illustration, we may refer to the need for a Court or a Judge's Order under the Banking Act, the Prevention of Corruption Act, the Financial and Anti Money Laundering Act and the Information and Communication Technology Act.

In view of what we have stated above, it is inconceivable that there can be such uncontrolled access to personal data in the absence of the vital safeguards afforded by judicial control. The potential for misuse or abuse of the exercise of the powers granted under the law would be significantly disproportionate to the legitimate aim which the defendants have claimed in order to justify the retention and storage of personal data under the Data Protection Act.

For all the reasons given above, we conclude that the plaintiff has been able to establish that the retention and storage of personal data under the Data Protection Act is not reasonably justifiable in a democratic society.

Conclusion

In view of our findings earlier in this judgment, we declare that:-

(1) the plaintiff has not established any breach of sections 1, 2, 4, 5, 7, 13, 15, 16 and 45 of the Constitution;

(2) the law which enforces the compulsory taking and recording of finger prints of a citizen of Mauritius for the purposes of his national identity card discloses an interference with the plaintiff's right against the search of his person guaranteed under section 9(1) of the Constitution;

(3) that law which enforces the compulsory taking and recording of fingerprints for the purposes of a national identity card constitutes a permissible derogation, in the interests of public order, under section 9(2) of the Constitution;

(4) the plaintiff has failed to establish that the compulsory taking of fingerprints for their insertion in the national identity card is not reasonably justifiable in a democratic society;

(5) the law providing for the storage and retention of fingerprints and other personal biometric data regarding the identity of a person constitutes a permissible derogation, in the interests of public order, under section 9 (2) of the Constitution;

(6) the provisions in the National Identity Card Act and the Data Protection Act for the storage and retention of fingerprints and other personal biometric data collected for the purpose of the biometric identity card of a citizen of Mauritius are unconstitutional.

The plaint with summons is otherwise dismissed. As plaintiff has been partly successful and in view of the importance of the constitutional issues raised, we make no order as to costs.

E. Balancy
Senior Puisne Judge

511

A.F. Chui Yew Cheong
Judge

A. A.Caunhye
Judge

29th May 2015

Judgment delivered by Hon. E. Balancy, Senior Puisne Judge

For Applicant : Me. Attorney K Bokhoreee
Me. S. Teeluckdharry, of Counsel
Me E. Mooneeapillay, of Counsel

For Respondents : State Counsel

512

Neutral Citation Number: [2015] EWHC 2092 (Admin)

Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
DIVISIONAL COURT

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 17/07/2015

Before :

LORD JUSTICE BEAN
and
MR JUSTICE COLLINS

Between :

THE QUEEN on the application of (1) DAVID DAVIS MP (2) TOM WATSON MP (3) PETER BRICE (4) GEOFFREY LEWIS	Claimants
- v -	
THE SECRETARY OF STATE FOR THE HOME DEPARTMENT	Defendant
-and -	
OPEN RIGHTS GROUP PRIVACY INTERNATIONAL THE LAW SOCIETY OF ENGLAND AND WALES	Interveners

Dinah Rose QC, Ben Jaffey and Iain Steele (instructed by Liberty) for the Claimants Mr Davis and Mr Watson
Richard Drabble QC, Ramby de Mello, Azeem Suterwalla and James Dixon (instructed by Bhatia Best) for the Claimants Mr Brice and Mr Lewis
James Eadie QC, Daniel Beard QC and Sarah Ford (instructed by Government Legal Department) for the Defendant
Jessica Simor QC and Ravi Mehta (instructed by Deighton Pierce Glynn) for Open Rights Group and Privacy International, intervening by way of written submissions
Tom Hickman (instructed by Legal Services Department, the Law Society) for The Law Society of England and Wales, intervening by way of written submissions

Hearing dates : 4-5 June and 9 July 2015

Lord Justice Bean :

This is the judgment of the court to which we have both contributed.

1. The claimants in three separately issued claims, which we heard together, apply for judicial review of the data retention powers in section 1 of the Data Retention and Investigatory Powers Act 2014 ("DRIPA"). Mr Brice and Mr Lewis, the claimants for whom Mr Drabble QC appeared, are concerned about the width of the powers to retain and gain access to their data on a number of grounds, including (but not limited to) the confidentiality of communications with solicitors. Mr Davis and Mr Watson, who are joint claimants in case CO/3794/2014, do so as members of the House of Commons who share those general concerns but also in addition have particular concerns about the confidentiality of communications to and from constituents. Mr Davis is Conservative MP for Haltemprice and Howden; Mr Watson is Labour MP for West Bromwich East.

2. Permission to seek judicial review was initially refused on the papers by Blake J but was granted at an oral hearing by Lewis J on 8th December 2014. Lewis J also permitted Open Rights Group and Privacy International to submit an intervention by way of written submissions (on terms that the interveners would bear their own costs). We granted an application by the Law Society made shortly before the hearing to intervene by way of written submissions on the same basis.

3. The challenge is to the validity of s 1 of DRIPA and the Regulations made under it as being contrary to European Union law, as expounded in the decision of the Grand Chamber of the Court of Justice of the European Union ("the CJEU") in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others* and the conjoined case of *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* delivered on 8th April 2014 and reported at [2015] QB 127. We shall refer to this decision as "*Digital Rights Ireland*".

4. At common law, Acts of the United Kingdom Parliament are not open to challenge in the courts. But the position under EU law is different. Decisions of the CJEU as to what EU law is are binding on the legislatures and courts of all Member States. The subtleties of the relationship between UK domestic courts and the European Court of Human Rights at Strasbourg arising, since 2000, from the duty under s 2(1) of the Human Rights Act 1998 to "take account" of the jurisprudence of that court, do not arise. The claimants (as a fallback to their EU law arguments) have pleaded an alternative claim for a declaration under s 4 of the HRA 1998 that s 1 of DRIPA is incompatible with their Convention rights; but this was scarcely mentioned in oral argument. Indeed, as will be seen later in this judgment, it was mainly counsel for the Home Secretary, not counsel for the claimants, who asked us to take account of the jurisprudence of the Strasbourg court in support of his arguments.

5. The present claims involve, as did *Digital Rights Ireland*, the CJEU's interpretation of Articles 7 and 8 of the Charter of Fundamental Rights of the EU. Article 7 provides:

> "Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 provides:

> "1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."

The first of these Articles is in identical terms to Article 8(1) of the ECHR, except that the word "correspondence" is replaced by "communications". The second has no counterpart in the ECHR.

6. In *Rugby Football Union v Consolidated Information Services Ltd (formerly Viagogo Ltd)* [2012] 1 WLR 3333 Lord Kerr of Tonaghmore JSC, with whom the other Justices of the Supreme Court agreed, said at paragraphs 27-28:-

> "The Charter was given direct effect by the adoption of the Lisbon Treaty in December 2009 and the consequential changes to the founding treaties of the EU which then occurred. Article 6(1) of the Treaty on European Union (TEU) now provides:
>
> > "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.
> >
> > The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties.
> >
> > The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions."
>
> Although the Charter thus has direct effect in national law, it only binds member states when they are implementing EU law - article 51(1). But the rubric, "implementing EU law" is to be interpreted broadly and, in effect, means whenever a member state is acting "within the material scope of EU law".....Moreover, article 6(1) of TEU requires that the Charter must be interpreted with "due regard" to the explanations that it contains."

7. The Secretary of State's Detailed Grounds of Defence are thus correct in stating at paragraph 38 that "the test of validity of the Act [DRIPA] and the 2014 Regulations is whether they are compliant with Articles 7 and 8 of the EU Charter and/or Article 8 ECHR." Data protection law has been within the scope of EU law for 20 years. The Data Protection Act 1998 was enacted to implement the Data Protection Directive (95/46/EC). The Explanations referred to in the Charter and printed in the Official Journal of the EU make it clear that Article 8 of the Charter was based on Article 286 of the Treaty establishing the European Community (as amended) and on the Data Retention Directive, among other sources. This is not a case in which any party has argued that Article 8 of the Charter lies outside the proper scope of EU law, although it will be seen that there is a dispute as to whether it covers access to data as well as retention.

8. Article 52(3) of the Charter provides:-

> "In so far as this Charter contains rights which correspond to rights guaranteed by the [ECHR], the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

9. The Secretary of State prays in aid the first sentence; the Claimants the second. As to the second, Mr Eadie submitted that it does not entitle the CJEU (or this court) to hold that the scope of anyone's rights has been extended by virtue of the Charter, since it was not intended to give fresh rights but to consolidate existing rights. This approach, he submitted, is confirmed by Protocol 30 to the EU Treaties, negotiated by the UK and Poland, which provides:-

> "The Charter does not extend the ability of the Court of Justice, or any court or tribunal of Poland or of the UK, to find that the laws, regulations or administrative provisions or action of Poland or of the UK are inconsistent with the fundamental rights, freedoms and principles that it reaffirms.
>
> In particular, and for the avoidance of doubt, nothing in Title IV of the Charter creates justiciable rights applicable for Poland or the UK except in so far as Poland or the UK has provided for such rights in the national law." [Title IV is not relevant in this case]

10. The precise scope of Protocol 30 is far from clear, since it only precludes the *extension* by the CJEU or domestic courts of their existing powers to find that UK laws are not in accordance with the Charter. It cannot be used to prevent the court from defining the extent of rights contained in the Charter which set out provisions within the material scope of EU law.

11. The extent of the State's powers to require the retention of communications data and to gain access to such retained data are matters of legitimate political controversy both in the UK and elsewhere. The Queen's Speech opening the new Parliament on 27 May 2015 indicated that "new legislation will modernise the law on communications data". To take one example from abroad, on 2 June 2015 the US Congress passed one

statute (the USA FREEDOM Act) restricting the data retention powers previously conferred by another statute passed in 2001 (the USA PATRIOT Act). It is not our function to take sides in this continuing debate, nor to say whether in our opinion the powers conferred by DRIPA are excessive or not. We have to decide the comparatively dry question of whether or not they are compatible with EU law as expounded by the CJEU in *Digital Rights Ireland*.

12. On 11 June 2015, a few days after the main hearing before us had concluded, the Government published "A Question of Trust", a 373-page report on the operation and regulation of investigatory powers by David Anderson QC, Independent Reviewer of Terrorism and Security Legislation. His report was rightly described by the Prime Minister in a statement to Parliament as thorough and comprehensive. We allowed the parties to make short written submissions to us about it.

Communications data

13. The phrase "communications data" does not include the content of a communication. Such data can be used to demonstrate who was communicating; when; from where; and with whom. They can include the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. They do not include the content of any communication: for example the text of an email or a conversation on a telephone. Communications data comprise three broad categories:

    (a) Subscriber data: information held or obtained by a communications service provider (CSP) in relation to a customer, for example their name, address and telephone number;

    (b) Service data: information relating to the use made by any person of a communications service and for how long, for example, itemised telephone records showing the date, time and duration of calls and to what number each call was made; and

    (c) Traffic data: data comprised in or attached to a communication by means of which it is being or may be transmitted, for example, who the user contacted, at what time the contact was made, the location of the person contacted and the location of the user.

14. Communications data are used by the intelligence and law enforcement agencies during investigations regarding national security and organised and serious crime. They enable investigators to identify members of a criminal network, place them in specific locations at given times and in certain cases to understand the criminality in which they are engaged. They can be used as evidence in court.

15. As the Home Secretary said in a statement to the House of Commons on 10 July 2014:

> "Communications data has played a significant role in every Security Service counter-terrorism operation over the last decade. It has been used as evidence in 95 per cent of all serious organised crime cases handled by the Crown Prosecution Service. And it has played a significant role in the investigation of many of the most serious crimes in recent time, including the Oxford and Rochdale child grooming cases, the murder of Holly Wells and Jessica Chapman and the murder of Rhys Jones. It can prove or disprove alibis, it can identify associations between potential criminals, and it can tie suspects and victims to a crime scene."

16. Similarly, in his March 2015 Report, the Interception of Communications Commissioner, Sir Anthony May, explained:

> "My inspectors identified that communications data was frequently relied on to provide both inculpatory and exculpatory evidence. The communications data acquired revealed suspects movements and tied them to crime scenes. It often led to other key evidence being identified or retrieved. Links to previously unidentified offenders and offences were revealed. Dangerous offenders were located and offences were disrupted with the assistance of communications data. Patterns of communication provided evidence of conspiracy between suspects. The data highlighted inconsistencies in accounts given by suspects and corroborated the testimony of victims. The data determined the last known whereabouts of victims and persons they had been in contact with. Similarly, communications data assisted to eliminate key suspects or highlighted inconsistencies in accounts given by victims."

EU legislation on data retention

The Data Protection Directive

17. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the Data Protection Directive") contained provisions designed to ensure the free movement of personal data between Member States and to protect individuals' fundamental rights and freedoms, in particular their right to privacy.

18. Article 3(2) provided that the Directive did not apply to the processing of personal data which fell outside the scope of Community law, and in any case to processing operations concerning public security, defence, State security (including the economic wellbeing of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

19. Article 13(1) preserved the right of Member States to enact domestic provisions to restrict the scope of the obligations and rights set out in the Directive where necessary

to safeguard inter alia national security; defence; public security; and/or the prevention, investigation, detection and prosecution of criminal offences.

20. Chapter IV of the Directive set out principles governing the transfer of personal data to third countries. By virtue of Article 25(1), such transfer could take place provided the third country in question ensured an "adequate level of protection" as defined in Article 25(2).

21. Article 28 of the Data Protection Directive required each Member State to provide for independent monitoring and oversight of the application within that Member State's territory of the provisions of the Directive.

Directive 97/66/EC

22. The retention and use of communications data was first addressed at EU level by Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector ("Directive 97/66/EC").

23. Article 1(3) of Directive 97/66/EC contained the same stipulation as Article 3(2) of the Data Protection Directive to the effect that it did not apply to activities which fell outside the scope of Community law, such as those provided for by Titles V and VI of the EU Treaty, or in any case to activities concerning public security, defence, State security or the activities of the State in areas of criminal law.

24. Article 14 of Directive 97/66/EC reiterated Article 13(1) of the Data Protection Directive in providing that Member States may adopt domestic legislative measures to restrict the rights laid down in the Directive where necessary inter alia to safeguard national security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences.

The e-Privacy Directive

25. Directive 97/66/EC was repealed and replaced by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("the e-Privacy Directive").

26. Again, Article 1(3) of the e-Privacy Directive provided that it did not apply to activities which fell outside the scope of Community law, or in any case to activities concerning public security etc. Following the pattern of the Data Protection Directive and Directive 97/66/EC, Article 15(1) authorised Member States to adopt domestic legislation to restrict the rights and obligations contained in the Directive, in the following terms:

> "Application of certain provisions of Directive 95/46/EC
>
> Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic

> society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use or the electronic communications system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

27. Article 5 of the e-Privacy Directive requires that the confidentiality of communications be ensured *except* when access is legally authorised in accordance with Article 15(1). This permits legislation to restrict the scope of the rights otherwise protected by the Directive "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. state security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [the Data Retention Directive]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in the paragraph."

The Data Retention Directive

28. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ("the Data Retention Directive") sought to harmonise the communications data retention arrangements across the EU.

29. The need for an EU-wide approach arose from an increasing recognition by the Member States of the importance of communications data for the investigation, detection and prosecution of crime, coupled with the differences between national data retention regimes which were creating barriers to free movement of services in the internal market. These matters are recorded in the recitals to the Data Retention Directive:

> "(5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.
>
> (6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and

location data to be retained and the conditions and periods of retention.

(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime...

(9)...Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure...

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive...

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty..."

30. The Data Retention Directive was adopted on the basis of Article 95 EC (now Article 114 TFEU), which gives the EU legislative competence to adopt harmonisation measures that have as their object the establishment and functioning of the internal market.

31. Article 1 of the Data Retention Directive emphasised this harmonising objective:

> "This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."

32. The Data Retention Directive specified the categories of data to be retained and imposed certain requirements relating to the security and storage of retained data. Article 6 imposed an obligation on each Member State to ensure that the specified communications data were retained by telecommunications providers for periods of not less than six months and not more than two years.

33. Article 4 of the Data Retention Directive provided that:

> "Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights."

Ireland v European Parliament and Council

34. In Case C-301/06 *Ireland v. European Parliament & Council* (ECLI:EU:C:2009:68; [2009] 2 CMLR 37) Ireland sought to argue before the CJEU that the Data Retention Directive was invalid and that it could not properly have been based on former Article 95 EC, because its principal focus was not the functioning of the internal market but the investigation, detection and prosecution of crime. That argument was rejected by the Grand Chamber of the Court of Justice. The Court observed that:

> "...the Community legislature may have recourse to Article 95 EC in particular where disparities exist between national rules which are such as to obstruct the fundamental freedoms or to create distortions of competition and thus have a direct effect on the functioning of the internal market".

35. It found that Article 95 EC was the correct legal basis for the Data Retention Directive, in particular because:

(a) "the differences between the various national rules adopted on the retention of data relating to electronic communications were liable to have a direct impact on the functioning of the internal market" and "such a situation justified the Community legislature in pursuing the objective of safeguarding the proper functioning of the internal market through the adoption of harmonised rules";

(b) the Directive amended the e-Privacy Directive, which was also based on Article 95 EC. In so far as amendment of that Directive was within the scope of Community (i.e. 'First Pillar') powers, the Data Retention Directive could not be based on (what was at the time) a 'Third Pillar' provision of the EU Treaty relating to police and judicial cooperation in criminal matters, without infringing the separation put in place by (what was at the time) Article 47 of the EU Treaty;

(c) the provisions of the Data Retention Directive were essentially limited to the commercial activities of communications service providers and did not govern access to, or use of, data by the police or judicial authorities of the Member States (paragraph 80 of the judgment). It regulated operations that were independent of the implementation of any police and judicial cooperation in criminal matters and harmonised "neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities. Those matters.....have been excluded from the provisions of that Directive, as is stated in particular in recital 25 to the preamble to, and Article 4 of, the Directive."

36. At paragraph 57 of its judgment the CJEU said:-

> "It must also be stated that the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006-24"

That challenge was to come in *Digital Rights Ireland*. Before coming to that case it is convenient to set out the relevant UK domestic legislation prior to 2014.

Domestic legislation

Data Protection Act 1998

37. As we have noted, the Data Protection Directive was implemented in the UK by the Data Protection Act 1998. Section 6 and Schedule 5 provide for independent oversight by the Information Commissioner. The eighth of the data protection principles listed in Schedule 1 to the Act, together with the derogations in Schedule 4 to the Act, implement Articles 25 and 26 of the Data Protection Directive concerning the transfer of personal data to third countries.

38. The safeguards in the Data Protection Act applied to access to communications data. However, there was no mandatory data retention regime. Security, intelligence and law enforcement agencies making use of communications data were obliged to rely solely on data routinely retained by communications companies for their own purposes.

Regulation of Investigatory Powers Act 2000 ("RIPA")

39. Chapter II of Part I of RIPA set out the access regime pursuant to which certain public authorities might obtain and use communications data. Access to communications data required an authorisation by a designated person of an appropriate grade within a

public authority with the requisite powers under RIPA. Section 22, headed "Obtaining and disclosing communications data", provided:-

> "(1) This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.
>
> (2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary—
>
> (a) in the interests of national security;
>
> (b) the purpose of preventing or detecting crime or of preventing disorder;
>
> (c) in the interests of the economic well-being of the United Kingdom;
>
> (d) in the interests of public safety;
>
> (e) for the purpose of protecting public health;
>
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
>
> (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
>
> (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State."

DRIPA amended s.22(2)(c) of RIPA by adding the proviso "so far as those interests are also relevant to the interests of national security". Some limited additional purposes were specified by paragraph 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010, which was itself amended in 2015.

Anti-terrorism, Crime and Security Act 2001

40. Following the terrorist attacks in the United States on 11 September 2001, the Anti-terrorism, Crime and Security Act 2001 put in place arrangements for the retention of communications data by communications providers pursuant to a voluntary code of practice so that they could be accessed by the security, intelligence and law enforcement agencies.

Privacy and Electronic Communications (EC Directive) Regulations 2003

41. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426) implemented the e-Privacy Directive in the United Kingdom.

Data Retention (EC Directive) Regulations 2007 and 2009

42. The Data Retention Directive was implemented in the United Kingdom with respect to fixed network and mobile telephony by the Data Retention (EC Directive) Regulations 2007 (S.I. 2007/2199) ("the 2007 Regulations"). The 2007 Regulations were superseded by the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859) ("the 2009 Regulations"), which contained additional provisions relating to internet access, internet telephony and email.

Regulation of Investigatory Powers (Communications Data) Order 2010

43. This statutory instrument set out the office holders designated for the purposes of chapter II of RIPA and thus permitted to grant authorisations or give notices under that statute. The same provisions are incorporated by reference into DRIPA. An example is that a police superintendent may give a notice in relation to traffic data or service data but a police inspector may give a notice in relation to subscriber data.

Digital Rights Ireland

44. In *Digital Rights Ireland* the CJEU held that the Data Retention Directive was invalid. The reasoning of the CJEU in *Digital Rights Ireland* is so central to the present case that we set it out in full in Appendix 1.

45. The invalidation of the Data Retention Directive by the CJEU put in doubt the legal basis for requiring the continued retention of communications data under the 2009 Regulations. Although the 2009 Regulations remained in force, they had been made under s. 2(2) of the European Communities Act 1972 to implement the Data Retention Directive and were already subject to a legal challenge that had been stayed pending the outcome of the *Digital Rights Ireland* case. We were told that following the *Digital Rights Ireland* judgment, some CSPs expressed the view that there was no legal basis for them to continue to retain communications data, and indicated that they would start to delete data that had been retained under the 2009 Regulations.

46. The absence of a clear legal power to require communications data to be retained threatened the ability of UK law enforcement and intelligence agencies to use communications data to investigate criminal activity and protect the public. The fact that DRIPA was a response to *Digital Rights Ireland* is apparent from the opening words of the long title of the statute, describing it as: "An Act to make provision, in consequence of a declaration made by the Court of Justice of the European Union in relation to Directive 2006/24/EC, about the retention of certain communications data……". Mr Regan's evidence notes that the Bill was fast-tracked through Parliament. It passed through all its stages in the House of Commons on 15 July 2014, was considered by the House of Lords on 16 and 17 July, and received the Royal Assent on 17 July.

The 2014 Act (DRIPA)

47. Section 1 of DRIPA provides as follows:

"Powers for retention of relevant communications data subject to safeguards

(1) The Secretary of State may by notice (a "retention notice") require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 (purposes for which communications data may be obtained).

(2) A retention notice may-

(a) relate to a particular operator or any description of operators,

(b) require the retention of all data or any description of data,

(c) specify the period or periods for which data is to be retained,

(d) contain other requirements, or restrictions, in relation to the retention of data,

(e) make different provision for different purposes,

(f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.

(3) The Secretary of State may by regulations make further provision about the retention of relevant communications data.

(4) Such provision may, in particular, include provision about-

(a) requirements before giving a retention notice,

(b) the maximum period for which data is to be retained under a retention notice,

(c) the content, giving, coming into force, review, variation or revocation of a retention notice,

(d) the integrity, security or protection of, access to, or the disclosure or destruction of, data retained by virtue of this section,

(e) the enforcement of, or auditing compliance with, relevant requirements or restrictions,

(f) a code of practice in relation to relevant requirements or restrictions or relevant powers,

(g) the reimbursement by the Secretary of State (with or without conditions) of expenses incurred by public telecommunications operators in complying with relevant requirements or restrictions,

(h) the 2009 Regulations ceasing to have effect and the transition to the retention of data by virtue of this section.

(5) The maximum period provided for by virtue of subsection (4)(b) must not exceed 12 months beginning with such day as is specified in relation to the data concerned by regulations under subsection (3).

(6) A public telecommunications operator who retains relevant communications data by virtue of this section must not disclose the data except-

(a) in accordance with-

(i) Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 (acquisition and disclosure of communications data), or

(ii) a court order or other judicial authorisation or warrant, or

(b) as provided by regulations under subsection (3).

(7) The Secretary of State may by regulations make provision, which corresponds to any provision made (or capable of being made) by virtue of subsection (4)(d) to (g) or (6), in relation to communications data which is retained by telecommunications service providers by virtue of a code of practice under section 102 of the Anti-terrorism, Crime and Security Act 2001."

48. Section 2 of the Act includes a number of definitions, including "relevant communications data", which means "communications data of the kind mentioned in the Schedule to the 2009 Regulations so far as such data is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned".

49. The purposes for which a notice to retain relevant communications data may be given pursuant to s.1(1) of DRIPA are those enumerated in s.22(2)(a)-(h) of RIPA, as set out above, with the amendment to s 22(2)(c) which we have noted.

50. Section 8(3) of DRIPA is a "sunset clause": it provides that the Act "is repealed" on 31 December 2016, thus putting the onus on Parliament to enact new primary legislation by that time.

51. Section 21 of the Counter-Terrorism and Security Act 2015 amended the definition of 'relevant' communications data to include data showing which internet protocol

address, or other identifier, belongs to the sender or recipient of a communication. That section came into force on 13 April 2015.

The Data Retention Regulations 2014

52. The Secretary of State made Regulations on 30 July 2014, following affirmative resolutions of both Houses, in exercise of the powers contained in s.1 of DRIPA.

53. Regulation 4 makes provision in respect of retention notices as follows:

> "4.— Retention notices
>
> (1) A retention notice must specify—
>
> (a) the public telecommunications operator (or description of operators) to whom it relates,
>
> (b) the relevant communications data which is to be retained,
>
> (c) the period or periods for which the data is to be retained,
>
> (d) any other requirements, or any restrictions, in relation to the retention of the data.
>
> (2) A retention notice must not require any data to be retained for more than 12 months beginning with—
>
> (a) in the case of traffic data or service use data, the day of the communication concerned, and
>
> (b) in the case of subscriber data, the day on which the person concerned leaves the telecommunications service concerned or (if earlier) the day on which the data is changed.
>
> (3) A retention notice which relates to data already in existence when the notice comes into force imposes a requirement to retain the data for only so much of a period of retention as occurs on or after the coming into force of the notice.
>
> (4) A retention notice comes into force when the notice is given to the operator (or description of operators) concerned or (if later) at the time or times specified for this purpose in the notice.
>
> (5) A retention notice is given to an operator (or description of operators) by giving or publishing it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator (or description of operators) to whom it relates."

54. Regulation 5 sets out the matters that the Secretary of State must take into account before giving retention notices:

> "5.— Matters to be taken into account before giving retention notices
>
> (1) Before giving a retention notice, the Secretary of State must, among other matters, take into account—
>
> (a) the likely benefits of the notice,
>
> (b) the likely number of users (if known) of any telecommunications service to which the notice relates
>
> (c) the technical feasibility of complying with the notice,
>
> (d) the likely cost of complying with the notice, and
>
> (e) any other impact of the notice on the public telecommunications operator (or description of operators) to whom it relates.
>
> (2) Before giving such a notice, the Secretary of State must take reasonable steps to consult any operator to whom it relates."

55. Regulation 6 requires the Secretary of State to keep a retention notice under review.

56. Regulations 7 and 8 impose obligations on public telecommunications operators who retain communications data, including: to secure its integrity and security; to protect it from accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure; to destroy the data so as to make it impossible to access if the retention of the data ceases to be authorised; and to put in place adequate security systems. Regulation 9 imposes a duty on the Information Commissioner to audit compliance with these requirements.

57. Schedule 1 specifies the types of communications data that may be retained under the Act, replicating the Schedule to the 2009 Regulations.

58. Regulation 10 of the Regulations makes provision for the issue of codes of practice.

Retention of Communications Data Code of Practice

59. The Retention of Communications Data Code of Practice came into force on 25 March 2015. It provides further guidance as to the procedures to be followed when communications data is retained pursuant to s.1 DRIPA and the Regulations.

Acquisition and Disclosure Code of Practice

60. The Acquisition and Disclosure of Communications Data Code of Practice issued in 2007 was revised with effect from 25 March 2015, inter alia to reinforce the independence of the authorising officer from the specific investigation for which the communications data is required. Paragraph 3.12 of the revised Code provides that

"designated persons must be independent from operations and investigations when granting authorisations or giving notices related to those operations".

61. In the case of communications data involving certain professions, the revised Code provides as follows:

> "3.72 Communications data is not subject to any form of professional privilege – the fact that a communication took place does not disclose what was discussed, considered or advised.
>
> 3.73 However the degree of interference with privacy may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.
>
> 3.74 Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of privacy, and clearly note when an application is made for the communications data of a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion. Particular care must be taken by designated persons when considering such applications. That such an application has been made must be recorded (see section 6 on keeping of records for more details)."

The scope of Article 15(1) of the e-Privacy Directive

62. One issue raised in the skeleton arguments, particularly that submitted on behalf of the first and second interveners, was that s1 of DRIPA was in breach of EU law on the simple grounds that it allows retention of traffic data for purposes other than those expressly permitted by article 15 of the e-Privacy Directive, namely "to safeguard national security (i.e. state security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences". Since the list of purposes permitted by s22(2) of RIPA, and therefore by s1 of DRIPA, goes beyond this list, it was submitted that the statute can be seen to be incompatible on its face without reference to the EU Charter or the judgment in *Digital Rights Ireland*. The argument was taken up by counsel for the claimants.

63. However, Mr Eadie drew our attention to the inclusion in article 15(1) of the e-Privacy Directive of a reference to article 13(1) of the Data Protection Directive; and to the fact that in *R (British Telecommunications PLC) v Secretary of State for Culture, Olympics, Media and Sport* [2012] Bus LR 1766 the Court of Appeal, following the decision of the CJEU in *Promusicae* (Case C-275/06), held that the grounds for derogation under article 15(1) of the e-Privacy Directive included the

purposes listed in article 13(1) of the Data Protection Directive. The claimants accept that this decision is binding on us but reserve the point should the present case go to the Supreme Court. We therefore need say no more about it.

Retention notices

64. The evidence before us does not include, even in a redacted form, the contents of any retention notice. In his evidence on behalf of the Secretary of State Paul Regan, Head of the Counter-Terrorism Legislation and Investigatory Powers Unit in the Home Office, states that the Home Office does not intend to publicise either the content of such notices or the identity of the CSPs to whom they are given. He explains:-

> "...This is because to do so would risk undermining national security and the prevention and detection of crime and for reasons of commercial confidentiality. To provide a confirmation or denial as to whether a notice has been given to a specific CSP or to disclose any details of such a notice would allow interested parties to determine the extent and scope of work in this area. This would provide an insight into what the limit or scope of operation capability might be. Information concerning operation capability in respect of law enforcement and national security is highly sensitive information. It would be of significant value to criminal or terrorist groups. If, for example, the Home Office were to confirm that no notice had been given to a particular company, criminals and terrorists may choose to use that company rather than companies they know or suspect could be subject to a notice."

65. Mr Eadie accepted that the consequence of this policy stance is that we should test the validity of DRIPA on the assumption that the retention notices issued under it may be as broad in scope as the statute permits, namely a direction to each CSP to retain all communications data for a period of 12 months. The case was argued on both sides on that basis. We shall refer in this judgment to a system under which the State may require CSPs to retain all communications data for a period as a "general retention regime".

66. It was also accepted on all sides that it is unnecessary for any of the Claimants to show that public authorities have in fact acquired their communications data. The ECHR said in *Weber and Saravia v Germany* (2008) 46 EHRR SE5 at [78]:

> "The Court further notes that the applicants, even though they were members of a group of persons who were likely to be affected by measures of interception, were unable to demonstrate that the impugned measures had actually been applied to them. It reiterates, however, its findings in comparable cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an

> interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them."

The Investigatory Powers Tribunal has adopted the same approach in this jurisdiction: see *Liberty v GCHQ and others* [2015] 3 All ER 142 at paragraph 4(ii).

Privilege

67. The Code of Practice issued by the Secretary of State states that communication data will not be subject to legal professional privilege since there will be no access to the contents of retained communications. The Law Society made written submissions which challenge the correctness of this statement. Reliance is placed on a dictum of Cotton LJ in *Gardner v. Irvin* (1878) 4 Ex D 49 at 83 where he said:-

> "I think that the plaintiffs are not entitled to have the dates of the letters and such other particulars of the correspondence as may enable them to discover indirectly the contents of the letters, and thus to cause the defendants to furnish evidence against themselves in this action".

This approach was confirmed by Vinclott J in *Derby v. Weldon (No 7)* [1990] 1 WLR 1156.

68. No doubt such an example of privilege would rarely arise. However, communications with practising lawyers do need special consideration. The same in our view can properly be said to apply to communications with MPs. The Code of Practice makes clear the need for such special attention.

The claimants' case on Digital Rights Ireland

69. The Claimants make numerous criticisms of DRIPA on the merits. As we have already observed, we are not concerned with those, but with whether s 1 of the Act is incompatible with the requirements of EU law as interpreted by the CJEU in *Digital Rights Ireland.* Ms Rose's skeleton argument suggested that the CJEU decided that data retention legislation, if it is to be compatible with EU law, must:

    i) restrict retention to data which relates to public security, and in particular restrict retention to a particular time period, a geographical area and/or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious criminal offences [paragraph 59];

    ii) provide for there to be exceptions for persons whose communications are subject to an "*obligation of professional secrecy*" (including Members of Parliament, lawyers and journalists) [58];

    iii) restrict access and use of the data to the purposes of prevention, detection or prosecution of defined, sufficiently serious crimes [60-61];

    iv) "*above all*" ensure that an independent administrative or judicial body carries out a prior review of decisions regarding access to the data on the basis of what is strictly necessary [62];

v) ensure destruction of the data when it is no longer required [67]; and

vi) ensure the data is kept within the EU [68].

70. In oral argument Ms Rose modified her stance on point (i). She accepted that the CJEU cannot have meant that CSPs can only lawfully be required to retain the communications data of "suspects or persons whose data would contribute to the prevention, detection or prosecution of serious criminal offences". Such a restriction would be wholly impracticable. Rather the Court must be understood to have held that a general retention regime is unlawful unless it is accompanied by an access regime which has sufficiently stringent safeguards to protect citizens' rights set out in Articles 7 and 8 of the Charter.

The defendant's case on Digital Rights Ireland

71. Mr Eadie submitted that in *Digital Rights Ireland* the CJEU:

i) did not explain why they thought it necessary to go beyond the jurisprudence of the Strasbourg court on the protection of ECHR Article 8 rights, and must therefore be understood not to have intended to do so;

ii) were not dealing with a challenge to any Member State's domestic legislation;

iii) could not have been laying down requirements for access regimes to comply with EU law, since in *Ireland v Parliament* the Court had held that access regimes were not the province of EU law;

iv) decided only that the Data Retention Directive taken as a whole was invalid, not that each specific aspect of it commented on in the judgment was non-compliant with the Charter.

72. Mr Eadie and his team, in their supplementary submissions following the publication of the Anderson report, cited Mr Anderson's observations at 5.78 of his report on *Digital Rights Ireland.* We set out paragraphs 5.77-5.79 in full:

> "5.77. The Grand Chamber of the CJEU is the apex of the judicial pyramid where EU law is concerned, and its conclusions are strictly binding. The extent to which current UK law gives effect to the requirements of *Digital Rights Ireland* is disputed in the MPs' case referred to at 5.75 above, which will be heard in the High Court in June 2015. In the circumstances, it would be inappropriate for me to venture an opinion on its legal compatibility.
>
> 5.78. There are however powerful arguments against an over-broad interpretation of the *Digital Rights Ireland* judgment. In particular:
>
> (a) What the Grand Chamber said about prior independent authorisation (5.68(f), above), seems to go further than the case law of the ECtHR but without explaining why. See, for example, *Kennedy v UK* (not cited by the Grand Chamber), in

which the ECtHR accepted prior authorisation of individual warrants by the Secretary of State even where the interception of content was concerned.

(b) Though the CJEU was prepared to describe data retention as a "*particularly serious*" infringement of fundamental rights, concrete examples of harm are not provided and are not immediately evident.[95] While there may be some for whom the retention of data "*is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*"(*Digital Rights Ireland*, para 37), the survey evidence suggests that this is putting it rather high.[96]

(c) There is a case for excluding the use of retained communications data in relation to the most trivial of offences (5.67(e) above). But if the mark for "*serious crime*" is set too high, damaging crimes will go needlessly unpunished and public confidence in law enforcement will be reduced.

(d) To limit retention to "*particular persons likely to be involved, in one way or another, in a serious crime*", and/or to "*persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences*"(*Digital Rights Ireland*, para 59), would not only reduce the effectiveness of data retention in identifying targets but would carry other risks, since to seek to apply such nebulous distinctions would be to court allegations of prejudice, profiling and unlawful discrimination.

5.79. The wider implications of the judgment also need to be reflected upon. Though *Digital Rights Ireland* did not concern the bulk interception of content, it is arguable that its principles (including in relation to prior independent authorisation) should apply in that area with at least the same force. Indeed the CJEU stated in terms that the bulk interception of content would be more intrusive, since unlike the Data Retention Directive it would affect the "*essence*" of the fundamental right to privacy (para 39). There may be implications also for other types of surveillance in relation to which types of self-authorisation are practised, in particular by the security and intelligence agencies. All this is subject to EU law being applicable: though to the extent that *Digital Rights Ireland* may in the future be adopted or followed by the ECtHR, that distinction will cease to matter."

The Strasbourg case law

73. We have already noted that it has not been (and could not sensibly be) argued that data protection falls outside the proper scope of EU law. Mr Eadie, however, placed reliance on the jurisprudence of the European Court of Human Rights (ECtHR), which he submitted is required to be applied under EU law and which has approved the UK's regime for access to communications data under RIPA.

74. Mr Eadie's starting point was Recital (2) to the e-Privacy Directive, which states:-

> "This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Article 7 and 8 of that Charter."

75. Clearly Article 7 of the Charter corresponds to Article 8 of the ECHR, and ECtHR jurisprudence is therefore directly material in interpreting it. Mr Eadie cited a number of cases from the ECtHR which concerned telephone tapping, retention of data or access to communications, starting with *Malone v. UK* (1985) 7 EHRR 14. As is the custom in ECtHR judgments, subsequent cases restate the applicable principles; so it is not necessary to refer in this judgment to all of them.

76. The most recent is the decision of a Chamber of the ECtHR in *Kennedy v. UK* (2011) 52 EHRR 4. The claimant had been convicted (he asserted wrongly) of manslaughter. Following his release from prison after serving his sentence, he had involved himself in campaigning against miscarriages of justice. The case before the ECtHR concerned the lawfulness of the use of the RIPA regime to intercept his communications. The Act required all warrants for such interception to have been issued (or, in cases of urgency, authorised) by the Secretary of State personally.

77. In paragraphs 151 to 154 the Court set out the relevant principles:-

> "151. The requirement that any interference must be "in accordance with the law" under Article 8 § 2 will only be met where three conditions are satisfied. First, the impugned measure must have some basis in domestic law. Second, the domestic law must be compatible with the rule of law and accessible to the person concerned. Third, the person affected must be able to foresee the consequences of the domestic law for him (see, among many other authorities, *Rotaru v. Romania*, cited above, § 52; *Liberty and Others*, cited above, § 59; and *Iordachi and Others*, cited above, § 37).
>
> 152. The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields (see *Malone*, cited above, § 67; *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116; *Association for European Integration*, cited above, § 79; and *Al-Nashif*, cited above, § 121). In its admissibility decision in *Weber and Saravia*, cited above, §§ 93 to 95, the Court summarised its case-law on the requirement of legal "foreseeability" in this field:

"93. ... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, inter alia, *Leander v. Sweden*, judgment of 26 August 1987, Series A no. 116], p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, inter alia, *Malone*, cited above, p. 32, § 67; *Huvig*, cited above, pp. 54-55, § 29; and *Rotaru)*. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, judgment of 25 March 1998, Reports 1998-II, pp. 542-43, § 72, and *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, Reports 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Malone*, ibid.; *Kopp*, cited above, p. 541, § 64; *Huvig*, cited above, pp. 54-55, § 29; and *Valenzuela Contreras*, ibid.).

94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, pp. 32-33, § 68; *Leander*, cited above, p. 23, § 51; and *Huvig*, cited above, pp. 54-55, § 29).

95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased

> or the tapes destroyed (see, inter alia, *Huvig*, cited above, p. 56, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, pp. 1924-25, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003)."
>
> 153. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court recalls that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see *Klass and Others*, cited above, §§ 49 to 50; and *Weber and Saravia*, cited above, § 106).
>
> 154. The Court has acknowledged that the Contracting States enjoy a certain margin of appreciation in assessing the existence and extent of such necessity, but this margin is subject to European supervision. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded (see *Kvasnica v. Slovakia*, no. 72094/01, § 80, 9 June 2009)."

78. The Strasbourg court decided that the scheme as set up by RIPA did not contravene Article 8 of the ECHR. Its reasons set out in paragraphs 166 and 167 can be summarised as acceptance of the protection provided by the Interception of Communications Commissioner in his role, which included protection of the public from wrongful access to their data, and the right of any individual who believed his communications were being accessed to make an application to the Investigatory Powers Tribunal.

79. The ECtHR has not considered a case which concerns general retention of communication data, as opposed to access to the data of a particular identified individual. Mr Eadie makes the point that access to the content of communications is more intrusive than access to communications data. But the ECtHR in *Kennedy* was considering only access, and whether it interfered with ECHR Article 8 rights. Different considerations apply to the retention regime and Article 8 of the Charter.

80. The protection of personal data is an aspect of the right to respect for private and family life set out in Article 8 of the ECHR and Article 7 of the Charter: and if Article 7 of the EU Charter were the only aspect of EU law in play, there would be force in the argument that the Strasbourg and Luxembourg courts should be expected to march

in step. However, Article 8 of the Charter clearly goes further, is more specific, and has no counterpart in the ECHR. We therefore reject Mr Eadie's argument that European law requires us to interpret *Digital Rights Ireland* so as to accord with the decisions of the ECtHR culminating in *Kennedy*.

81. In any event there is an obvious difference between the cases. Mr Eadie is right to say that interception of content is more intrusive than access to communications data. But on the other hand a case about the interception of material relating to one individual, pursuant to a case-specific warrant signed personally by a Secretary of State, does not in our view assist much in interpreting the judgment of the CJEU in *Digital Rights Ireland* relating to a general retention regime on a potentially massive scale.

82. As Mr Anderson says in the passage of his report cited by Mr Eadie, the CJEU did not explain why they went further than the case law of the ECtHR. But it was their prerogative not to explain. EU law does not permit a national court to disregard a ruling of the CJEU on the grounds that it is inadequately explained or inadequately reasoned.

No challenge in Digital Rights Ireland to domestic legislation

83. Mr Eadie is also right to say that the CJEU in *Digital Rights Ireland* only ruled on the validity of the Directive. That was what the Irish and Austrian referring courts had asked it to do: it was not asked to consider domestic legislation. But this is an argument which elevates form over substance. The issue was not, as it had been in *Ireland v European Parliament and Council*, a technical (though important) one about the jurisdictional basis of the Directive. Rather it was whether the EU legislature had "exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter" (paragraph 69 of the judgment), and the Court's answer was that it had. It must follow, in our view, that an identically worded domestic statute would have been found to have exceeded the same limits. Similarly, at paragraph 66 the Court had held that the Directive "does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data". Again, it must follow that in the view of the CJEU a domestic statute in identical terms would have had the same failings.

Was the Court pronouncing on the access regime as well as the retention regime?

84. Retention for the purpose of possible access is in itself an interference with rights under Articles 7 and 8 of the Charter and Article 8 of the ECHR: see paragraph 29 of the judgment in *Digital Rights Ireland*. In *Liberty v UK* (2009) 48 EHRR 1 the ECtHR observed at paragraph 56:-

> "Telephone, facsimiles and e-mail communications are covered by the notions of 'private life' and 'correspondence' within the meaning of [ECHR] Article 8. The court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This necessarily strikes at freedom of communication between users of the

> telecommunications services and thereby amounts in itself to an interference with the exercise of the applicant's rights under Art.8 irrespective of any measures actually taken against them."

85. In paragraphs 58 and 59 of *Digital Rights Ireland* the Court was not indicating that communications data can *only* be retained if they relate to particular geographical areas, or to particular individuals likely to be involved in serious crime. It was identifying the width of the Directive, which imposed no limits on the power to retain. But the Court was not, as we read the judgment, purporting to lay down any particular limitations on that power, as opposed to conditions of access. To have done so would, apart from being to some extent impracticable, have been inconsistent with the Court's clear conclusion in paragraph 44 of the judgment that "the retention of data for the purpose of allowing the competent national authorities to have possible access to those data.....genuinely satisfies an objective of general interest."

86. Counsel for the Secretary of State reminded us that in *Ireland v European Parliament and Council* the CJEU had held that the provisions of the Data Retention Directive were "essentially limited to the activities of service providers", and did not govern or seek to harmonise provisions on access to data or the use thereof by the police or judicial authorities of the Member States, such matters being excluded from the Directive (paragraphs 80 and 83). Accordingly, Mr Eadie submitted, it is beyond the scope of EU law to lay down minimum provisions for a data access regime, and in *Digital Rights Ireland* the CJEU cannot have been intending to do so.

87. We do not know whether the CJEU in *Digital Rights Ireland* agreed with all that their predecessors had said about the Data Retention Directive in *Ireland v Parliament*. The previous decision is referred to and considered in detail in the Opinion of Advocate General Cruz Villalón in *Digital Rights Ireland* (see paragraphs 42-46, 81-88, 121 & 124). Yet in the judgment of the Court it is not even mentioned. It seems to us quite extraordinary that in the second case to consider (albeit in different respects) the validity of the same Directive the CJEU said nothing about its reasoning in the first such case, decided only five years earlier.

88. What *is* clear, however, is that in *Digital Rights Ireland* the CJEU held that the Directive was invalid; that it infringed the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter; and that it failed to provide sufficient safeguards against unlawful access to and use of retained data by public authorities. Paragraphs 57-59 of the judgment concern retention; but paragraphs 60-67 of the judgment concern access. Mr Eadie did not submit that the latter are simply to be discarded or ignored. It was not clear to us how, on the Secretary of State's case, those paragraphs of the judgment are to be treated.

89. The solution to the conundrum, in our view, and the *ratio* of *Digital Rights Ireland*, is that legislation establishing a general retention regime for communications data infringes rights under Articles 7 and 8 of the EU Charter *unless* it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights.

Was the Court laying down any (and if so what) specific minimum requirements for compatibility with EU law?

90. Mr Eadie was of course right to submit that the *decision* which the CJEU had to make in *Digital Rights Ireland* was binary, namely whether the Directive was valid or invalid. We do not accept that the case is authority for nothing more than that overall verdict, any more than we interpret the judgment as meaning that each criticism or concern which the Court expressed involves a fatal flaw in the legislation. But some points are made with such emphasis that we understand the Court to have laid down mandatory requirements of EU law.

91. We put the following observations by the Court in this category:

(a) The protection of the fundamental right to respect for private life requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. Consequently the legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards sufficient to give effective protection against the risk of abuse and against any unlawful access to and use of that data (paragraphs 52 and 54);

(b) Any legislation establishing or permitting a general retention regime for personal data *must* expressly provide for access to and use of the data to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences (paragraph 61);

(c) "*Above all*", access by the competent national authority to the data retained *must* be made dependent on a prior review by a court or an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued, and which intervenes following a reasoned request of those authorities (paragraph 62). [emphasis added]

92. The supplementary submissions on behalf of the Defendant also make the point that whereas the Anderson report is the product of a year's work in gathering and assessing a large volume of material, that "can be contrasted with the complete absence of evidence before the CJEU in *Digital Rights Ireland* as to any individual Member State's domestic data retention and access regimes". It is not clear to us how much information the CJEU were given about the domestic regimes in Ireland and Austria: but even if the answer is "little or none", it does not detract from the binding nature of the conclusions of the CJEU as to what is required in order for legislation to comply with the Charter.

93. We repeat that our task is not to say what safeguards we would ourselves consider necessary or desirable, but to interpret the words of the CJEU. Nevertheless, we should mention some arguments addressed to us about practicalities.

94. The requirement that access to and use of the data must be strictly restricted to the purpose of preventing and detecting "precisely defined serious offences" or of conducting criminal prosecutions relating to such offences does not mean that access must be limited to the data of people suspected to have committed serious crime. Mr Regan (in paragraph 56 of his statement) said that investigations against serious criminals would be 'severely hampered if data could only be retained where the data

was already known to be linked to serious crime.' This is because investigation is often needed of lower level individuals whose activities are not themselves considered to have been serious.

95. In some circumstances a wholly innocent person's data might be accessed in order to assist in the detection of serious crime by others. The need for access to data is not limited to data directly attributable to particular individuals suspected of having committed serious crimes. It can be needed in relation to serious crime committed by anyone. The status of the individual in respect of whom access is sought cannot determine whether such access should be permitted, although it may of course be material in considering whether such access is indeed necessary.

96. As to the definition of serious crimes, the CJEU makes it clear that this is a matter for national legislatures, so long as the relevant offences are precisely defined and can properly be regarded as serious. Parliament has not found it difficult in previous criminal justice legislation to draw up schedules of offences considered serious for various purposes and it is unlikely to be difficult to so again in the present context.

97. Turning to the question of the need for judicial or independent review, Mr Eadie drew our attention to reservations expressed by Sir Anthony May, the Interception of Communications Commissioner (ICC). These resulted from consideration of how the requirement of judicial approvals for local authority communications data requests imposed by the Protection of Freedoms Act 2012 was working. Sir Anthony and his predecessor Sir Paul Kennedy had consistently been of the view that the requirement for judicial approval would not be likely to lead to improved standards or 'have any impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data'. But their criticisms were essentially of lack of training of magistrates, instances of a failure by magistrates to carry out proper scrutiny of applications, failure by the Ministry of Justice to introduce an electronic system to avoid delay and the requirements in some cases for payment of fees.

98. The provisions of RIPA, as applied by DRIPA, require (as we have noted above) that an application for access to communication data must be considered by a senior person who is independent of the investigation. There is already a need for there to be a written request for approval. The need for that approval to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome. The views of Sir Anthony May and Sir Paul Kennedy are entitled to respect; but if EU law requires independent approval, as we are satisfied it does, that must be put in place. It is not for us to devise the appropriate system. As to the question of what level of consideration should be given to applications involving access to data involving communications with lawyers, Members of Parliament, or journalists, that too is not for us to determine. We only observe that such cases do require special consideration.

99. We add the important proviso that the requirement of prior approval relates to access, not to retention. We see no reason why the exercise of the power to retain should need prior independent approval, and we do not understand the CJEU to have held that it does.

Retention in the EU

100. In paragraph 68 of its decision in *Digital Rights Ireland*, the court referred to the lack of proper control in that the Directive did not require the data to be retained within the EU. It is obviously important that EU Member States should pass on information which materially assists in dealing with serious crime or terrorism. Equally, such exchange of information should be available to friendly powers outside the EU. But there is a requirement that any provision of information outside the EU should require the Member State supplying it to be satisfied that safeguards which correspond to those required by EU law are in force. It would to say the least be unfortunate if a failure by the UK to comply with EU law as set out by the court should inhibit other Member States from disclosing material information. We do not consider, however, that on a proper interpretation of *Digital Rights Ireland* it is necessary for restrictions on passing on information about communications data outside the EU to be embodied in statute.

Reference to the CJEU

101. In the course of the hearing before us on 4 and 5 June 2015 we asked leading counsel on each side whether their clients were asking us to refer the present case to the CJEU and received negative replies. But on 22 June we received from the solicitor for Mr Davis and Mr Watson a copy of a reference by the Stockholm Administrative Court of Appeals to the CJEU lodged on 4th May 2015 (case C/203/2015) in the case *Tele2 Sverige AB* of the following questions:-

> "Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime compatible with Article 15(1) of Directive 2002/58/EC [the E-Privacy Directive] taking account of Articles 7, 8 and 15(1) of the Charter?
>
> If the answer to question 1 is in the negative, may retention nevertheless be permitted where access by the national authorities to the retained data is determined as described below; security requirements are regulated as described below; and all relevant data are to be retained for six months ... and subsequently deleted.....?"

102. The court was considering the provisions of three Swedish statutes: they have some similarities to DRIPA but are by no means identical to it.

103. It appears that the Stockholm court making the reference took the view, as we do, that the judgment of the CJEU in *Digital Rights Ireland* does not prohibit the retention of traffic data provided that the requirements of the e-Privacy Directive are met and there is otherwise no infringement of EU law. However, the referring court noted that the parties had differing views as to how the judgment of the CJEU was to be interpreted and wished "to have a clear answer to the question whether the EU court of justice carried out a weighted assessment in that judgment of the scope of retention and the provisions governing data access, period of retention and security".

104. On 23 June 2015 the Treasury Solicitor sent a letter to us, subsequently developed by way of skeleton argument, requesting a reference to the CJEU. The claimants,

understandably, opposed the late request to refer the case to Luxembourg. We heard oral argument on this issue on 9 July 2015.

105. The Swedish case is not the only decision of a domestic court of another Member State concerning *Digital Rights Ireland* to which we have been referred. Mr Welch, solicitor for Mr Davis and Mr Watson, has referred us to four decisions in other Member States, three of them by Constitutional Courts, holding their country's communications data legislation invalid without finding it necessary to make a reference to the CJEU: the Constitutional Court of Slovenia on 3 July 2014; the Constitutional Court of Romania on 8 July 2014; the District Court of The Hague on 11 March 2015 and the Constitutional Court of Belgium on 11 June 2015. Some of the translations we have of those judgments are unofficial, and the details of each country's laws under scrutiny are of course not identical: but the general theme is clear.

106. Mr Eadie relied on the judgment of Sir Thomas Bingham MR in *R v Stock Exchange ex p Else Ltd* [1993] QB 534 at 545, where he said:

> "I understand the correct approach in principle of national courts (other than a final court of appeal) to be quite clear: if the facts had been found and a community law issue is critical to the court's final decision, the appropriate course is ordinarily to refer the issue to the Court of Justice unless the national court can with complete confidence resolve the issue itself. In considering whether it can, with complete confidence resolve the issue itself, the national court must be fully mindful of the differences between national and Community legislation, of the pitfalls which face a national court venturing into what may be an unfamiliar field, of a need for uniform interpretation throughout the community and of the great advantages enjoyed by the Court of Justice in construing Community instruments. If the national court has any real doubt, it should ordinarily refer."

107. It seems to us that in *Else* the Master of the Rolls primarily had in mind issues of EU law which have arisen without there being an existing judgment of the CJEU giving that court's ruling on them. The *dicta* are less obviously applicable where the CJEU has pronounced judgment and the domestic court is being asked to interpret what it meant. In *Trinity Mirror v Commissioners of Customs and Excise* [2001] 2 CMLR 33 Chadwick LJ cited the above passage from *Else* and continued:

> "52. But it is, I think, important to have in mind, also, the observations of the Advocate-General (Mr Francis Jacobs QC) in Case C-338/95, *Wiener SI GmbH v. Hauptzollamt Emmerich.* The question which he thought it necessary to address is stated at paragraph 10 of his Opinion:
>
> ... whether it is appropriate—and especially whether it is still appropriate today, in view of developments which I shall mention below—for the Court to be asked

> to rule in every case where a question of interpretation of Community law may arise.
>
> He identified the matter which was of practical concern to the Court of Justice, at paragraph 15:
>
> "Any "application" of a rule of law can be regarded as raising a question of "interpretation"—even if the answer to the question of interpretation may seem obvious. Every national court confronted with a dispute turning on the application of Community law can refer a question which, if more or less properly phrased, this Court is bound to answer after the entire proceedings have taken their course. That will be so even where the question is similar in most respects to an earlier question; the referring court (or the parties' lawyers) may always seek to distinguish the facts of the cases. It will be so even where the question could easily, and with little scope for reasonable doubt, be answered on the basis of existing case law; again the facts may be different, or it may be that a particular condition imposed in earlier case law gives rise to a new legal argument and is regarded as needing further clarification. The net result is that the Court could be called upon to intervene in all cases turning on a point of Community law in any court or tribunal in any of the Member States. It is plain that if the Court were to be so called upon it would collapse under its case-load."
>
> The solution is "a greater measure of self-restraint on the part of both the national courts and the Court of Justice"—see paragraph 18. Where the national court is not a court of last resort, a reference will be most appropriate where the question is one of general importance and where the ruling is likely to promote the uniform application of the law throughout the European Union. A reference will be least appropriate where there is an established body of case law which could readily be transposed to the facts of the instant case..."

108. A reference was refused in *Trinity Mirror* because, as Chadwick LJ put it at [55], "the question of principle has been decided by the Court of Justice and a national court or tribunal can now act in the light of that decision".

109. We take the same view in this case. The Claimants' objections to a reference are well founded for several reasons.

110. Firstly, we are not the domestic court of last resort. We do not doubt that the questions raised in this case are of general importance, but we do not consider that to refer the present case to Luxembourg is likely to promote the uniform application of the law throughout the EU: the CJEU has given general guidance already in *Digital Rights*

Ireland, and it is apparent from the cases cited to us that Member States have different regimes governing the retention of and access to communications data.

111. Secondly, we are not persuaded that the fact that the Swedish court has referred the issue to Luxembourg means that we should do the same. It might just as well be said on the other side that we should follow our colleagues in Slovenia, Romania, the Netherlands and Belgium in holding our domestic legislation to be in breach of EU law without making a reference.

112. Thirdly, the request is made far too late. DRIPA was enacted on 17 July 2014. These proceedings were issued on 13 August 2014. Permission for judicial review was granted on 8 December 2014. If a request was to be made on the grounds that the judgment in *Digital Rights Ireland* was so difficult to comprehend that only the CJEU itself could say what it meant, that application should have been made at an early stage; certainly not after the conclusion of a two day oral hearing, with the parties having incurred substantial costs.

113. Fourthly, and perhaps most importantly of all, DRIPA contains a sunset clause which, as we have noted, means that the Act will expire on 31st December 2016. The CJEU typically takes two years or more to answer a question referred to it for a preliminary ruling. It is most unlikely that an answer to a reference made now would be received before DRIPA has expired, or (far more probably) has been repealed and replaced by a new statute. Either way, the answer would have become academic.

Conclusion

114. The application for judicial review succeeds. The Claimants are entitled to a declaration that section 1 of the Data Retention and Investigatory Powers Act 2014 is inconsistent with European Union law in so far as:

a) it does not lay down clear and precise rules providing for access to and use of communications data retained pursuant to a retention notice to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences; and

b) access to the data is not made dependent on a prior review by a court or an independent administrative body whose decision limits access to and use of the data to what is strictly necessary for the purpose of attaining the objective pursued.

Remedy

115. On 10 July we sent paragraphs 1-114 above to counsel as a draft judgment and invited submissions in writing on remedy.

116. The Secretary of State's submissions ask us to go no further than a declaration; and to suspend any order we do make pending appeal. Mr Eadie relies on *R(Chester) v Secretary of State for Justice* [2014] AC 271, a challenge to the UK's ban on voting by convicted prisoners. The claimants sought to rely *inter alia* on EU law. Lord Mance JSC, giving the leading judgment, said that EU law does not incorporate a right to vote parallel to that recognised by the ECHR. But he added that even if it had,

the Supreme Court would not have granted any relief beyond a declaration. The statutory scheme was complex and it was not for the court to devise an alternative.

117. The Claimants propose an order for disapplication, suspended until 1 January 2016, to give time for compliance. As counsel for Mr Davis and Mr Watson put it in their submissions (with which counsel for Mr Brice and Mr Lewis agree):

> "The Claimants accept that Parliament will need to be afforded a reasonable opportunity to legislate for proper safeguards..... Despite its unlawfulness, the Claimants do not invite the Court to order that the entire DRIPA regime falls with immediate effect. The Claimants are anxious to ensure that serious criminal investigations are not impeded, and that the legislation necessary to resolve the defects in the current situation is not enacted with the same unfortunate haste that DRIPA was."

118. Ms Rose refers to the decision of the Supreme Court given on 29 April 2015 in *R (ClientEarth) v Secretary of State for Environment, Food and Rural Affairs* [2015] UKSC 28. The Secretary of State admitted that the UK was in breach of the air quality standards required by Article 13 of the Air Quality Directive (2008/50/EC). The High Court and Court of Appeal considered that this was a matter for the Commission, not the national courts. All relief was refused. The Supreme Court granted a declaration recording the UK's breach of EU law and made a reference to the CJEU as to (among other things) whether it should order further relief. The CJEU held that national courts must take "*any necessary measure, such as an order in the appropriate terms*" to ensure compliance with EU law (§58).

119. When the case returned to the Supreme Court, they granted a mandatory order requiring the production of air quality plans designed to end the breach, subject to a time limit for production and with liberty to apply. The Supreme Court had "*no hesitation in rejecting*" the submission that mandatory relief was unnecessary (§29). The Court concluded that "*we would... be failing in our duty if we simply accepted* [the Secretary of State's] *assurances without any legal underpinning... the new Government, whatever its political complexion, should be left in no doubt as to the need for immediate action to address this issue*" (§30).

120. The *ClientEarth* case is a significant and recent case on remedies in the UK courts for breaches of EU law. It does not lay down a rule that disapplication or mandatory relief, even with a reasonable time for compliance, must always be the appropriate remedy, but it gives a steer which in our view cannot be ignored.

121. We consider that an order for disapplication is appropriate, but that a date of 1 January 2016 for it to come into effect is too soon. The Government has already announced its intention to legislate in the current session of Parliament to replace DRIPA (as it must, given the sunset clause). Subject to any view different from ours taken by a higher court, it will no doubt seek to ensure that the new statute, unlike section 1 of DRIPA, is compliant with EU law. The courts do not presume to tell Parliament for how long and in what detail Bills should be scrutinised, but it is right to say (to put it no higher) that legislation enacted in haste is more prone to error, and it would be highly desirable to allow the opportunity of thorough scrutiny in both Houses. Moreover, if the route chosen for compliance with part (b) of the declaration

is authorisation by an independent administrative body, that body would have to be appointed after the passing of the new Act and be ready to start work by the time it comes into effect. All this would, we think, take longer than five months.

122. We will make an order disapplying s 1 of DRIPA to the extent that it permits access to retained data which is inconsistent with EU law in the two respects set out in our declaration, but suspend that order until 31 March 2016. The order will be that s 1 is disapplied after that date:

(a) in so far as access to and use of communications data retained pursuant to a retention notice is permitted for purposes other than the prevention and detection of serious offences or the conduct of criminal prosecutions relating to such offences; and

(b) in so far as access to the data is not made dependent on a prior review by a court or an independent administrative body whose decision limits access to and use of the data to what is strictly necessary for the purpose of attaining the objective pursued.

123. In their submissions on remedy following receipt of our draft judgment counsel for the Defendant raised for the first time the question of whether access to retained data for national security reasons is within the scope of EU law. This was not raised in the oral or written arguments previously addressed to us and we decline to allow it to be raised at this late stage. Whether national security cases should have different provisions for authorisation of access to communications data will no doubt be the subject of careful thought when the new legislation is being drafted.

Costs

124. Counsel and solicitors acting for Mr Davis and Mr Watson, to their very great credit, have acted *pro bono*, and pursuant to an agreement reached with the Government Legal Department they do not seek a *pro bono* costs order. In their case, therefore, there will be no order as to costs. Mr Brice and Mr Lewis are legally aided: it is accepted that in their case the Defendant must pay their costs, with the usual order for detailed legal aid assessment. The interveners will bear their own costs in accordance with the terms of the orders allowing them to intervene.

Permission to appeal

125. The Secretary of State seeks permission to appeal. Plainly the public importance of the case justifies the grant of permission, as the Claimants accept. We are prepared to grant permission subject to the condition in the case of Mr Davis and Mr Watson, who do not have the protection of a legal aid certificate, that the Defendant shall not be entitled to seek an order against them for costs either in this court or on appeal.

126. We express our gratitude to leading and junior counsel and solicitors for all parties for the exemplary assistance we have received in this case.

APPENDIX

Judgment of the CJEU in *Digital Rights Ireland* paragraphs 23-71

Consideration of the questions referred

The second question, parts (b) to (d), in Case C 293/12 and the first question in Case C 594/12

23. By the second question, parts (b) to (d), in Case C 293/12 and the first question in Case C 594/12, which should be examined together, the referring courts are essentially asking the Court to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter.

24. *The relevance of Articles 7, 8 and 11 of the Charter with regard to the question of the validity of Directive 2006/24*

25. It follows from Article 1 and recitals 4, 5, 7 to 11, 21 and 22 of Directive 2006/24 that the main objective of that directive is to harmonise Member States' provisions concerning the retention, by providers of publicly available electronic communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter.

26. The obligation, under Article 3 of Directive 2006/24, on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raises questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter.

27. In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

28. Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

29. In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.

30. The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (Cases C 92/09 and C 93/09 *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 47).

31. Whereas the references for a preliminary ruling in the present cases raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter.

32. In the light of the foregoing considerations, it is appropriate, for the purposes of answering the second question, parts (b) to (d), in Case C 293/12 and the first question in Case C 594/12, to examine the validity of the directive in the light of Articles 7 and 8 of the Charter.

Interference with the rights laid down in Articles 7 and 8 of the Charter

33. By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, as the Advocate General has pointed out, in particular, in paragraphs 39 and 40 of his Opinion, derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.

34. To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that

effect, Cases C 465/00, C 138/01 and C 139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 75).

35. As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.

36. Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., *Leander v. Sweden*, 26 March 1987, § 48, Series A no 116; *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.

37. Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.

38. It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General's Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

39. *Justification of the interference with the rights guaranteed by Articles 7 and 8 of the Charter*

40. Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

41. So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.

42. Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because

Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

43. As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.

44. It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest (see, to that effect, Cases C 402/05 P and C 415/05 P *Kadi and Al Barakaat International Foundation v Council and Commission* EU:C:2008:461, paragraph 363, and Cases C 539/10 P and C 550/10 P *Al-Aqsa v Council* EU:C:2012:711, paragraph 130). The same is true of the fight against serious crime in order to ensure public security (see, to that effect, Case C 145/09 *Tsakouridis* EU:C:2010:708, paragraphs 46 and 47). Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.

45. In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.

46. It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.

47. In those circumstances, it is necessary to verify the proportionality of the interference found to exist.

48. In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (see, to that effect, Case C 343/09 *Afton Chemical* EU:C:2010:419, paragraph 45; *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 74; Cases C 581/10 and C 629/10 *Nelson and Others* EU:C:2012:657, paragraph 71; Case C 283/11 *Sky*

Österreich EU:C:2013:28, paragraph 50; and Case C 101/12 *Schaible* EU:C:2013:661, paragraph 29).

49. With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).

50. In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

51. As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

52. That assessment cannot be called into question by the fact relied upon in particular by Mr Tschohl and Mr Seitlinger and by the Portuguese Government in their written observations submitted to the Court that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General's Opinion.

53. As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

54. So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C 473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).

55. In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.

56. Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99).

57. The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, *S. and Marper v. the United Kingdom*, § 103, and *M. K. v. France*, 18 April 2013, no. 19522/09, § 35).

58. As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

59. In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

60. Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

61. Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons,

contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

62. Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

63. Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

64. In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

65. Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

66. Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

67. It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in

the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

68. Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

69. Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

70. In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C 614/10 *Commission v Austria* EU:C:2012:631, paragraph 37).

71. Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

72. In those circumstances, there is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter.

73. Consequently, the answer to the second question, parts (b) to (d), in Case C 293/12 and the first question in Case C 594/12 is that Directive 2006/24 is invalid.